

## 1.2.2 NPAC/SMS Functionality

In the decade and a half since the inception of the NPAC, the system has evolved to offer a wide array of capabilities that benefit the provider community. As the NPAC Administrator during this entire period, Neustar has aggressively and responsibly fostered the advancement of new or improved functionality within the NPAC system. Further, Neustar maintains a vision for the NPAC into the future to continue this record of constant improvement.

The NPAC/SMS is a key component of the NPAC service and has evolved significantly over the last 15 years. NPAC/SMS functionality is developed in partnership with the Industry through various committees under the auspices of the NANC (for example, the LNPA WG).

In this section we describe the functionality that enables NPAC transactions, administrative functionality required to operate the service, and new functionality for the next term that are either proposed by Neustar or referenced in the RFP with the potential to improve value for the Industry.

<p><b>Functionality That Enables NPAC Transactions</b></p>	<ul style="list-style-type: none"> <li>• Subscription Version Processing</li> <li>• Facilitation of Industry Processes and Obligations</li> <li>• Support for National Number Pooling</li> </ul>
<p><b>Administrative Functionality</b></p>	<ul style="list-style-type: none"> <li>• Mass Update and Mass Port</li> <li>• Billing</li> <li>• Reporting</li> </ul>
<p><b>New Functionality for the Next Term</b></p>	<ul style="list-style-type: none"> <li>• Proposed Enhancement:                             <ul style="list-style-type: none"> <li>○ New NPAC Portal</li> </ul> </li> <li>• RFP Required Enhancements:                             <ul style="list-style-type: none"> <li>○ Security-Related Information</li> <li>○ Support of IP Version 6</li> <li>○ Elimination of NPAC/SMS Support of non-EDR</li> </ul> </li> <li>• Future Considerations:                             <ul style="list-style-type: none"> <li>○ Automation of Processes Between PAS and NPAC</li> <li>○ Combining steps for intra-SP ports</li> <li>○ Inter-carrier Communications</li> <li>○ PSTN to IP Transition</li> </ul> </li> </ul>

## 1.2.2.1 Functionality that Enables NPAC Transactions

### Subscription Version Processing

The majority of code in the Security-Related Information provides functionality that enables NPAC/SMS transactions. Records created in the NPAC/SMS by the users are called subscription versions (SV). SV processing can be divided into four main categories:

1. Enforcement of business rules
2. Data validations
3. Dissemination of data
4. Synchronization

### Enforcement of NPAC/SMS Business Rules

Processing an NPAC/SMS transaction is a complicated process that considers thousands of potential scenarios and invokes various business rules based on the combination of scenarios involved. Just a few of the factors that must be considered include portability type (Inter-provider, Intra-Provider), existence of pool blocks, single-TN versus ranged-TN operations, support of optional capabilities (e.g. pseudo-LRN, optional data fields), timer settings for the involved carriers, and business hour calculations (days of the week, holidays).

The NPAC/SMS uses a complex rules engine to manage over a thousand business rules that can interact in, literally, millions of ways. Integrating a new business rule to implement a new Industry rule requires a unique mix of skills, including a deep understanding of NPAC transactions, an understanding of the specific new feature, and intimate knowledge of how the rules engine works within the NPAC/SMS to determine the impact of the new rule on existing rules. Neustar has developed this expertise over the course of many years in its role as the NPAC Administrator.



The following five business rules: timers, conflict status, first port notification, snapback, and code recovery, serve as examples of the complexity of enforcing the NPAC/SMS business rules.

### **Enforcement of NPAC Business Rules: Timers**

The timers used by the NPAC to determine when to shift control of the port from the old SP to the new SP are referred to as the T1 and T2 timers. At the start of the T1 interval, at the end of the T1 interval (the start of the T2 interval), and at the end of the T2 interval, the NPAC generates a notification to the old SP to remind it that a pending SV has been created by the new SP and to request a reaction (concurrency or objection to the impending port). There are three sets of T1/T2 timers: two sets ("long" and "short") are selected in advance by the Service Provider. Each Service Provider selects either of the timers for port-out transactions and either of the timers for its port-in transactions. These two selections become part of the Service Provider's NPAC/SMS profile. A third set of timers, referred to as "Medium Timers" is imposed on a porting transaction when the old SP determines that the port meets the FCC's One-Day Porting criteria.

The set of T1-T2 "short" timers involves a pair of one-hour intervals and typically is selected by wireless SPs. The set of T1-T2 "long" timers involves a pair of nine-hour intervals and typically is selected by wireline SPs. The longer interval is selected by wireline SPs to accommodate the added complexity of having to assign outside plant to implement service for their customers. The medium timers are a pair of three-hour intervals. Unless the medium timer has been determined by the old SP to apply to the port, the NPAC looks at the port-out timer shown on the old SP's profile and the port-in timer shown on the new SP's NPAC profile and selects the longer to determine how long the old SP remains in control absent the old SP reacting to the NPAC/SMS notification about the pending SV creation.

The timers run during NPAC/SMS "business hours" and "business days." The NPAC/SMS is available for use at all times, except during maintenance intervals, but the timers run only during "business hours." The SP selects either Sunday through Saturday or Monday through Friday for its business days. The Sunday-Saturday business days have business hours of 9:00 a.m. to 9:00 p.m., in the predominant time zone of the region. The Monday-Friday business days have business hours of 7:00 a.m. to 7:00 p.m., Central time. The SP's selection of business days/hours is noted on its NPAC profile. The business days/hours choice is independent of the short/long timers choices. Wireline SPs typically choose the Monday-Friday set while wireless SPs typically chose the Sunday-Saturday set.

When a port meets the FCC's criteria for a One-Day Port, the old SP invokes the medium timers, indicating the choice when it submits its matching "pending SV create" request to NPAC/SMS. The NPAC then ignores the business days/hours and long/short timer settings on the NPAC/SMS profile for the two SPs involved in the port and uses the medium timers:

- T-1/T-2 timers are each three hours
- Business days are Monday through Friday
- Business hours are 7:00 a.m. to midnight, in the region's predominant time zone

The new SP is not obligated to request a next day due date even though the One-Day Porting scenario requires that it be allowed.

#### ***Enforcement of NPAC Business Rules: Conflict***

When the new SP sends its "create pending SV" request to the NPAC/SMS, the NPAC/SMS sends a notification to the old SP. Thus if the LSR never made it to the SP actually serving the number, the NPAC/SMS notification serves as an alert that something is wrong. Likewise, if the old SP received the LSR, but has not issued its FOC, the NPAC/SMS notification serves as an alert that a port is being planned even without a FOC having been issued. Because the old Service Provider now is aware of the porting record being created in the NPAC/SMS, the old SP may have time to prevent or at least delay the port until it can contact the new SP to work out the problem.

The NPAC/SMS process allows the old Service Provider to put a pending port into "Conflict", thus preventing the new Service Provider from activating the port for 6 hours (or sooner, if the old SP removes the conflict). In cases where there has been no LSR received or no FOC issued, the old SP can put the pending SV record into conflict and prevent activation for an indefinite period. The design of the NPAC/SMS enforces the Industry's rules allowing the old SP to retain control of a port for a defined interval. The delay interval values also are defined by Industry.

In addition to the T1-T2 timer process described above, the old SP can extend its control of a port by setting the conflict flag in its "old SP pending SV create" message to "false." For both long and short timer cases, this extends the interval by six hours from the time NPAC/SMS receives the conflict indication. If the port involves a "medium timers" scenario, this extension is 2 hours. Once the interval expires, the new SP can remove the conflict and proceed with the port.

On occasion, the new SP may send its LSR to the wrong old SP or may fail to send it altogether. Should that new SP attempt to create a pending SV record, in anticipation of porting a telephone number away from the old SP, the NPAC/SMS (routinely) sends a notification to the old SP to say that a pending SV has been created and to request the corresponding old SP "create pending SV request" message be generated. The old SP, realizing no LSR was received, can send its matching "create pending SV" request with conflict indicated and the conflict "cause code" marked "50" (no LSR received). These indicate to the NPAC/SMS that the pending SV should be placed into a Conflict state and remain there until the old SP removes the conflict. The same conflict sequence could occur if the scenario were that the old SP received the LSR, but had not yet issued its FOC. In this case, the conflict cause code would be "51" (no FOC issued).

#### ***Enforcement of NPAC/SMS Business Rules: First Port Notification***

Some SPs do not establish translations in their networks when an NPA-NXX code is defined as portable and instead wait for the first port to occur in the NPA-NXX (or for the first thousand block to be created and assigned to a switch different from the one to which the NPA-NXX is assigned). The NPAC/SMS broadcasts a first-port notification when it receives the "create pending SV" request and prevents activation of the SV or block for five business days. The Industry requires this delay to enable those carriers that have not yet prepared their network to recognize the NPA-NXX code is portable to update their switch translators and begin doing data base dips for calls to numbers in the code.

#### ***Enforcement of NPAC/SMS Business Rules: Snapback***

When a consumer abandons a number he has ported, the current SP is not permitted to use the number for another of its customers and must return it to the original SP, after providing intercept services. This is called snapback. This is accomplished by deleting the NPAC/SMS record of the ported number. When a ported number record is deleted, the NPAC/SMS notifies the code-assignee (or block assignee, if a pooled block is involved) that the number is being returned to its inventory. The NPAC message includes the date the number was removed from active service, as indicated to the NPAC/SMS by the SP returning the number, thus enabling the code (or block) assignee to apply an appropriate aging interval. After the snapback message is sent, the NPAC/SMS broadcasts a delete message to all the LSMSs.

#### ***Enforcement of NPAC/SMS Business Rules: Code Recovery***

The introduction of LNP has also impacted the NPA-NXX code recovery process, where a code is assigned to a Service Provider and then later is returned to the NANPA code pool. Before the introduction of LNP, a recovered code was not contaminated, i.e., all 10,000 telephone numbers associated with it would be available for use by the next code assignee. However, a code that is defined as portable, or pooling enabled, that is recovered after it has been assigned, is likely to have had numbers ported from it. If the code is returned to the NANPA, and no action is taken to clear out the ported number records, the recovered code will not be pristine. When the code is later re-assigned, the new code assignee inadvertently may cause double assignments of telephone numbers that already are in service as ported numbers served by other SPs. To protect the code recovery process, the NPAC/SMS will

not allow deletion of network data when subordinate TN-level data exists, i.e., when there are ported numbers. Contaminated NPA-NXX codes are not returned to the NANPA pool until the NPAC's telephone number-level records are cleaned out. Because code recovery often involves a defunct SP, there may be no one available to agree to the deletion of the defunct SP's NPAC/SMS records. In these cases, the NANPA obtains written direction from the state regulator, requesting that the NPAC delete the defunct SP's code record and any associated records that must be deleted to allow the code's deletion. As a result of the NPAC's action, the recovered code contains the full 10,000 numbers for use by the new code-assignee when the code eventually is reassigned.

### **Data Validation**

Beyond enforcing Industry-defined porting processes, the NPAC/SMS validates the data it receives before completing the transaction and making the data available for dissemination. Data validations can be divided into format validations, verifying that format of the data provided conforms to Industry practices, and relationship validations, verifying the data provided against other NPAC data, Industry standards, and data from other sources such as NECA and NANPA.

#### ***Data Validation: Format Validations***

One type of format validation verifies the structure of the data; specifically number of characters and whether they are numbers letters or both. Examples are an LRN, which must be 10 numeric characters; an NPA-NXX code, which must be 6 numeric characters; a Destination Point Code, which must be 9 numeric characters; and a SPID, which must be 4 alphanumeric characters.

Another type of format validation involves compliance with Industry rules, such as confirming a Subsystem Number is present when a Destination Point Code is present or that the Destination Point Code entry conforms to common channel signaling (SS7) address range restrictions.

#### ***Data Validation: Relationship Validations***

Relationship validations involve verifying the data provided against existing data, such as whether the LRN entered on the ported number record exists and is associated with the New Service Provider involved in the record. Other examples are whether the value entered in the AltSPID or Last AltSPID field is a valid SPID in the NPAC's customer data, whether the value entered as the SV Type is among the defined SV Type values, and whether the NPA-NXX of the porting telephone number shown on the record exists in the NPAC's network data.

Somewhat more complex relationship validations involve confirming the SPID from which the number is being ported actually is the Service Provider currently serving the telephone number. This validation requires the NPAC/SMS to determine whether there is a ported number record already for the telephone number and, if so, to confirm the SPID associated with that record represents the "porting from" Service Provider shown on the "porting to" Service Provider's port request. If no ported number record exists, the NPAC/SMS then must check to see whether the telephone number is part of a thousand block associated with the "porting-from" Service Provider's SPID. And failing to find such a thousand block record, the NPAC must then determine whether the telephone number's NPA-NXX code is associated with the "porting from" Service Provider's SPID.

More complex validations check for relationships such as whether the Destination Point Code used is among those the Service Provider has listed as its valid DPC codes for use on its NPAC/SMS records. Another of these complex validations occurs when a Service Provider attempts to open an NPA-NXX code in the NPAC/SMS network data. Before the code can be opened, the NPAC/SMS determines to what Operating Company Number (OCN) the North American Numbering Plan Administrator (NANPA) has assigned the NPA-NXX code. That OCN then is compared with the list of OCNs associated with the SPID of the Service Provider attempting to open the code. The NPAC/SMS also confirms the code is being opened in the proper region. In two NPAC regions, this proper-region determination must be done at the rate area level because the regional boundary does not exactly track the state boundary, making it necessary to handle one NPA in two regions. Table 1.2.2-1 provides a summary of some of the validations performed by the NPAC/SMS.

**Table 1.2.2-1. Examples of Validations**

Field	Validation
<b>Simple Format Validation</b>	
LRN	must be 10 numeric characters
NPA-NXX	must be 6 numeric characters
DPC (SS7)	9 numeric characters
SPID	must be 4 alpha numeric
<b>Compliance with Industry Rules</b>	
DPC	must be accompanied by SSN entry
SSN	when present, must be 000
LRN	must be same LATA as TN's LATA
First port in NPA-NXX	5 business day delay before activation permitted
LRN	must be open in network data
LRN	must be network data owned by new SP
altSPID	must exist as SPID in customer data
Last altSPID	must exist as SPID in customer data
SV type	must be selected from defined values
NPA-NXX	must be open in network data
old SP SPID	accurately refers to current SP
DPC	must be known to be valid for SP creating record
NPA-NXX	SP SPID must be associated with code's OCN
NPA-NXX	allow open only in region serving the NPA *
<b>Network Data Relationships Tracked</b>	
OCN	OCNs associated with a SPID
DPCs	DPCs associated with a SPID

Field	Validation
NPA-NXX	NPA-NXXs associated with a SPID
NPA-NXX-X	NPA-NXX-Xs associated with a SPID
LRN	LRNs associated with a SPID
LATA	LATA associated with each NPA-NXX
NPA	NPAs associated with each region
SP Type	each SPID's SP type
Customer Name	Customer name associated with each SPID

*\* NPAC region boundary crosses state line in Kentucky, so proper region to open an NPA-NXX code is validated at the rate area level*

**Dissemination of Data**

Once the NPAC/SMS has applied its processing rules on a request and updated its internal database, it must disseminate this information to the LSMS and SOA systems. Real-time broadcasting is the primary mechanism for this dissemination. Most broadcasts are sent to the subtending LSMSs, though some go to the SOAs as well.

During the porting process, the NPAC/SMS acts as a hub, connecting pairs of Service Providers (SPs) that are coordinating the transfer of a telephone number. As each party performs a step in the process, the NPAC/SMS issues real-time notifications to their SOA systems to keep all parties abreast of the progress and make them aware of their obligations. Notifications are issued for object creation (port initiation), attribute value changes, status changes, and timer expirations. Though most NPAC/SMS messages to SOAs involve information pertinent to a single SOA, some NPAC/SMS transmissions are broadcasts to all SOAs; for example, the creation of SPIDs, NPA-NXXs, and the dash-X representation of pooled blocks.

NPAC/SMS users connect a system called a Local Service Management System (LSMS) for receiving and propagating NPAC/SMS transactions in their systems and networks. NPAC/SMS transactions are updates to the Industry on changes in status related to telephone numbers. These changes in status can be a move from one switch to another, one Service Provider to another, information for a non-ported TN different from that associated with the TN's NPA-NXX code, assignment of numbering resources (pooled blocks, NPA-NXX codes) to a Service Provider, as well as hundreds of other status changes. Once a transaction is validated and updated in the NPAC/SMS database, a broadcast of the SV is sent to NPAC/SMS users through the LSMS interface. The Service Provider's LSMS updates network databases and operations support systems. They can also distribute the data in turn to their clients, such as smaller SPs that cannot justify operating an LSMS system.

In the case of an NPA split, the NPAC/SMS broadcasts an "add" of the new-NPA versions of the NPA-NXX codes impacted by the NPA split when the split is entered into the NPAC/SMS. At the end of the Permissive Dialing Period, the NPAC/SMS broadcasts a "delete" of the old-NPA versions of the NPA-NXX codes impacted by the NPA split.

### **Synchronization**

One can think of the LNP Ecosystem as fundamentally a complex distributed database. The NPAC/SMS itself maintains the master copy of the LNP data and one of its primary goals is to ensure that remote systems have an accurate copy of that data. To this end, synchronization with remote systems is critical and the NPAC/SMS provides many layers of mechanisms to ensure consistency.

#### ***Synchronization: Recovery***

Local systems are not always online, and from time to time are not able to process messages correctly due to a variety of platform issues. The NPAC/SMS implements a feature called recovery that allows a local system to retrieve messages they have missed due to such a problem. The recovery process can be done for a specific time frame, or the system can ask the NPAC/SMS to deliver accumulated message that it has missed (this is called "Send What I missed" or SWIM recovery).

In the Security-Related Information rather than using recovery, the NPAC/SMS will retransmit messages that either could not be delivered or were not responded to. This simplifies the interface, reducing the burden on local system implementers.



#### ***Synchronization: Failed Lists and Resend***

When an SV or pooled block broadcast is received by an LSMS, it sends an acknowledgement to the NPAC/SMS. The NPAC/SMS keeps track of the LSMS responses for each broadcast. After a predefined interval, any LSMS that has not acknowledged the broadcast is placed on a "failed list." Each night, during a period of low transaction volume, the NPAC/SMS resends the broadcast to any LSMS that is on the failed list. For modify broadcast failures, the NPAC/SMS notes whether the LSMS failure was due to a "no record" rejection and for those casts sends a create message rather than rebroadcasting the modify transaction.

#### ***Synchronization: Bulk Data Downloads***

Bulk Data Downloads (BDD) provides data extracts from the NPAC/SMS to local systems requesting them. Local systems retrieve the BDD files from the NPAC/SMS and can use the files to validate their own database, re-populate their database after a loss of data, or build the initial database for a new system.

There are several different types of BDD files, based on the type of data they represent. There are BDD files for Subscription Versions, Pooled Blocks, DashX, NPA-NXX, LRN, and Service Provider. For each of these files, the BDD can be generated with an "active view" that includes currently active objects, or with a "latest view of activity" that captures all activity (including deletions and modifications) within a specified time frame.

We also provide a BDD for SOA notifications. This is available based on a specific time-frame and contains only notifications for the provider requesting the data.

***Synchronization: Audits***

The NPAC/SMS also supports audits of the LSMSs. With the audit feature, the NPAC/SMS queries one or more LSMSs, and compares the results of these queries with its own data, issuing corrective downloads as necessary. Audits can be initiated for a single TN, a TN range, or for a time range, and can be initiated by a SOA system or by the NPAC Administrators. The NPAC/SMS issues random audits as part of its housekeeping processing as a proactive consistency measure.

***Synchronization: Query***

Users can initiate queries to the NPAC/SMS and use the results to reconcile their systems. Responses are provided immediately. Queries can be for any data in the NPAC/SMS including TNs, ranges of TNs, SPIDs, DPC/SSNs, etc.

**Facilitation of Industry Processes and Obligations**

Because the NPAC/SMS is an authoritative database for TN administration it must support various functions that impact numbering as well as various entities that rely on numbering data. The NPAC/SMS has software that supports:

- Mergers and acquisitions of communications companies—SPID migrations
- Area code splits—recognition of dual NPAs for TNs
- Reseller identification—altSPID, last altSPID
- Administrative services that rely on NPAC—LEAP and WDNC
- IP routing—URI

**Mergers and Acquisitions**

The NPAC/SMS facilitates mergers and acquisitions through SPID migrations, a process that allows the SPID associated with the ported telephone numbers, thousand blocks, LRNs, and NPA-NXX codes to be changed without requiring that the data be broadcast to the LSMSs. Instead, the NPAC/SMS distributes information that allows the migrating records to be identified. The record changes are then made independently by each SOA and LSMS operator and by the NPAC/SMS during a regular NPAC/SMS maintenance window.

The NPAC/SMS offers on-line tools for both Service Providers and NPAC Administrators to define and manage these migrations. The tool implements the workflow of the migration, ensuring that both Service Providers in the migration have concurred with the activities. During the concurrence phase, automated e-mails are sent directly to the involved providers. After the migration is approved, automated emails are sent to all providers. The system also automatically validates the migration on a daily basis, and generates preliminary data files, making them available for providers at the FTP site. On the date of the migration, the system automatically cancels any pending subscription versions involved in the migration, provides reports to SPs impacted by the cancelled SVs, initiates message delivery and data updates for on-line migrations, and delivers files to Service Providers' FTP sites with instructions for handling the SPID migration off-line.

### **Area Code Splits**

The NPAC/SMS also performs automated processing for NPA splits. The system accepts data files from industry sources that describe NPA split activity. When a new split is added to the system, the NPAC/SMS broadcasts all the codes involved with the split, but with their new NPAs. During the Permissive Dialing Period, the NPAC/SMS automatically translates incoming requests—queries, ports etc., changing references to the old NPA to the new NPA. At the end of the Permissive Dialing Period, the NPAC/SMS broadcasts a delete of the old-NPA versions of all the codes involved in the split.

### **Reseller Identification**

There are instances where NPAC/SMS data can reflect information pertinent to the provider behind a PSTN Service Provider. For example, a "class 2 interconnected VoIP" provider must rely on its PSTN partner as a source of telephone numbers and to act as a PSTN gateway. It also must rely on its PSTN partner to create information in the NPAC/SMS database to identify it as the serving provider for the telephone number as well as to indicate other information pertinent to the service arrangement. Neustar has augmented the NPAC system to allow for the optional provisioning of reseller information through the "altSPID" optional field. This field is used to identify the VoIP provider that is actually providing telephone service for the number. If the telephone number involved were native to the PSTN partner's switch, i.e., not ported, then the PSTN partner would need to perform an intra-SP port at the NPAC/SMS to establish the number record in the NPAC/SMS database. If the telephone number already were ported, the PSTN partner would need to modify the NPAC/SMS record to populate the altSPID field. If the VoIP provider were prepared to accept calls directly in the form of internet traffic, the PSTN partner could indicate on the NPAC/SMS record that the "SV type" is "class 2 interconnected VoIP."

### **Administrative Services That Rely on NPAC**

The NPAC/SMS provides additional services to satisfy the needs of law enforcement to be able to accurately and immediately identify the ownership of any telephone number. These functionalities include access to additional interfaces such as Interactive Voice Response and Web and API access.

The NPAC system provides an additional service to satisfy the needs of Telemarketers and Collection Agencies to avoid placing calls to wireless numbers using automatic dialers and recorded messages, which is expressly prohibited by the FCC.

### **IP Routing**

The NPAC system supports the transition from TDM (PSTN) to non-TDM (IP) inter-carrier call routing. As the PSTN transition to IP unfolds, it will be necessary for every TN assigned to an ISP customer to be associated with both an LRN and a URI. The NPAC/SMS record for TNs and blocks includes fields for VoIP URI, SMS URI, and MMS URI.

## Support for National Number Pooling

Number Pooling is a process that is vital to the country because it conserves scarce numbering resources. Pooling is implemented using NPAC/SMS functionality. Neustar has evolved support for number pooling to a system that is fully aware of pooling and the pooled block lifecycle. The NPAC/SMS has many features incorporated specifically to support number pooling which can be integrated with the Pooling Administration System (PAS). Specifically, the NPAC/SMS and PAS can communicate electronically to exchange information on pooling operations that need to be executed in the NPAC/SMS and automatically reflect said completion in PAS. This will result in increased accuracy and timeliness.



Another evolution regarding Pooled Block processing concerns LSMS support for pooled blocks. At the inception of number pooling, not all LSMS systems supported the concept of pooled blocks, also known as Efficient Data Representation (EDR). EDR is a technique to represent 1,000 consecutive numbers as a single record, for example 703-571-3 represents the numbers 3000-3999 associated with the 703-571 NPA-NXX. As a result, the NPAC had to broadcast 1000 SVs to non-supported LSMS systems in lieu of the pooled block. Recently, the Industry achieved 100% support for Pooled Blocks, leading to a request for SOW 86 to remove support for non-EDR LSMS systems. Neustar complies with the requirement from RFP Section 7.1.3 to eliminate non-EDR support for SOA and LSMSs.



The NPAC/SMS still must support some non-EDR features, such as the ability to respond to an NPAC user's query for an individual pooled number. Although not a part of the EDR functionality, Neustar remains prepared to provide a Bulk Data Download (BDD) that includes individual number data for pooled numbers in cases where the customer is not yet able to process the now-standard EDR BDD.



### 1.2.2.2 Administrative Functionality

As the LNPA, Neustar needs certain administrative functionality to provide a high level of service to our users. To this end we have:

- Developed a tool to update large volumes of NPAC/SMS data (MUMP)
- Implemented a billing capability
- Deployed a reporting function for the Industry

#### Mass Update Mass Port (MUMP)

Service Providers often have a need to port large volumes of numbers in a controlled manner. For various operational reasons, executing these projects over the SOA interface is inefficient. The MUMP subsystem was developed to provide the tools and processes to manage such projects.

The initial version of MUMP allowed for updates of only existing records and could be used only by NPAC personnel. Over the course of many years, MUMP has evolved into a very complex subsystem that supports all types of portability operations (create, release, activate, modify, disconnect, and cancel).

MUMP allows a user to express operations as a "job". It uses a system of quotas and priorities to ensure that all work is done in an orderly fashion at reasonable transaction volumes and includes a dashboard to project completion dates for each job. The feature is available for both Service Providers and NPAC personnel. Jobs can be defined in

terms of a list of TNs or as a query. The NPAC Portal can upload spreadsheets, breaking the data up into separate jobs as required.

Many options are available to control the execution of the job, including an ability to control the start time and to suppress notifications that normally would be generated. Several types of reports are available to monitor the progress and results of each job.

### **Billing**

Billing for the NPAC service has changed substantially over time. Fortunately, the system was designed modularly to accommodate these changes.

The NPAC system can generate all data necessary to track system usage in a variety of ways to facilitate billing processes. The NPAC/SMS logs all transactions, recording the type of operation, the telephone number(s), Service Provider, and date/time. A module extracts this information into a separate repository where it can be summarized and reported. Another module implements the actual generation of customer bills based on the current contract stipulations.

The billing code within the NPAC/SMS is tested with every major release and results are provided to an independent auditor.

### **Reports**

The NPAC/SMS provides a wide array of user-generated reports. From within the NPAC Portal, users can generate Standard Reports on the following types of data:

- Subscriptions
- SPIDs and User names
- Network data (NPA-NXX, NPA-NXX-X, LRN, NPA Splits)
- Number pooling
- Audits
- Notifications
- Security data
- Transactions

These reports include report-specific filters to target the desired data. The reports can be scheduled to run periodically. The NPAC Portal also provides the ability to generate Ad-Hoc reports on subscription versions. In these reports, the user can specify the fields desired and a complex filter can be created. Additionally, NPAC personnel provide reports to the Industry or to the NAPM LLC. Examples of these reports include:

- Standard reports, such as the customer's NPAC Profile
- Ad Hoc reports, which are individually designed to meet customer request
- Results of MUMP projects, such as completion counts and failed transactions details
- Results of SPID migrations, such SPID-specific reports of pending SVs canceled in support of the migration
- Bulk data download (BDD) reports (active and delta) to establish or re-build LNP databases
- Root cause analyses (RCAs), to describe root cause of service interruptions
- Monthly "billable" transactions
- Monthly "billable" transactions, broken into p-LRN and conventional categories

### 1.2.2.3 New Functionality for the Next Term



#### Proposed Enhancements: NPAC Portal

Neustar has a record of consistent investment into the NPAC user experience, understanding that thousands of people across the Industry rely on the NPAC to accomplish critical business functions, from supporting customer port requests to network maintenance to number inventory administration. We also recognize that the LNPA is both a trusted resource for information regarding numbering policy and a common hub for collaboration and issue resolution between Service Providers and their partners. For these reasons, in 2011 Neustar, working with the Industry, implemented a complete technical and functional overhaul of the NPAC.com website, an improvement which received high marks from all user types.

As usage of the NPAC grows in volume, scope, and complexity, further automation and optimization of the NPAC experience is required. To that end, Neustar is planning continued investment into the NPAC's online interfaces—specifically, the creation of a single NPAC Portal (highlighted in Exhibit 1.2.2-1) which will be a one-stop shop and provide access to reports, billing information, secure and authenticated access to NPAC regions etc. The NPAC/SMS Portal will reduce NPAC User expenses by consolidating existing screens and interfaces, streamlining access to critical reports and Industry knowledge, and by automating customer support tasks.

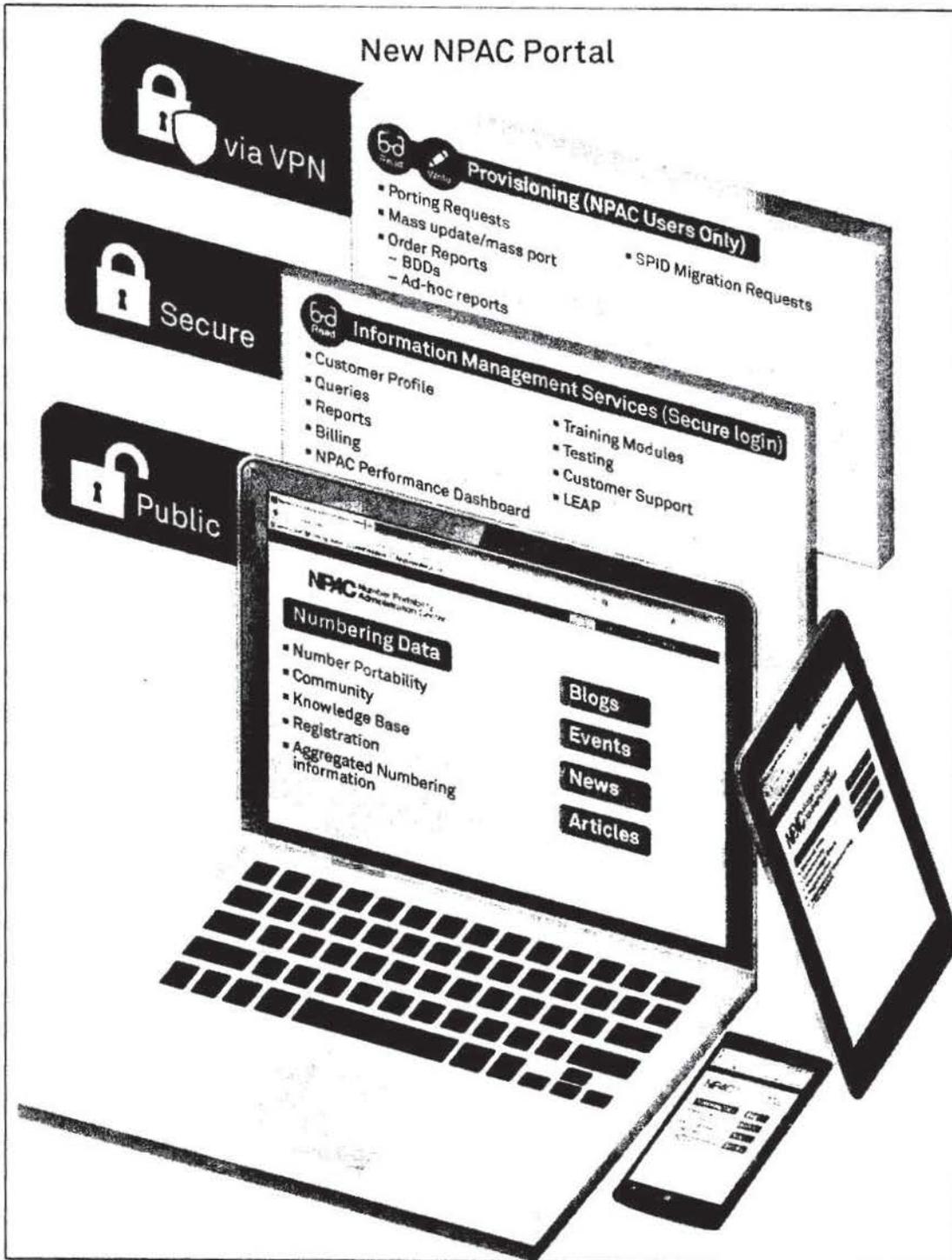


Exhibit 1.2.2-1: The new NPAC Portal, available via computer, smartphone, or tablet, provides NPAC users more valuable capabilities and a streamlined experience.

The NPAC portal will be designed and implemented in partnership with the LNPA WG and the NAPM LLC prior to the start of the next NPAC contract term, with the following guiding principles in mind:

- Operational efficiency and ease of use
- Security and user authorization/authentication
- Effective Industry collaboration and communication
- Access to business-critical information

**NPAC Portal: Operational Efficiency and Ease of Use**

The NPAC portal and all its functions should be accessible via an online interface securely accessible over the Internet. A single, unique, cross-regional user ID and password will be assigned to each authorized individual accessing the NPAC with the aim of eliminating the need for swivel-chair operations and reducing the number of logins required for an individual user.

All porting functions supported by the NPAC/SMS will be available through the NPAC portal, as they are today via the existing NPAC LTI. Added to the interface will be integrated, context-sensitive help, describing not only the system behavior and recommended usage, but also relevant Industry standards, best practices, and policy. The portal will also permit real-time, chat-based interaction with experts at the NPAC help desk for those users requiring additional assistance.

As part of the design process for the user interface itself, given the complexity of information and processes supported by the NPAC, Neustar will convene dedicated user group meetings for the Industry in collaboration with the LNPA Working Group and will make available experts in human factors to consult with the Industry on the most efficient usage models.

**NPAC Portal: Security and User Authorization/Authentication**

Confidentiality of NPAC data and user behavior, along with verified authorization for porting activity, remain the highest priority for the user community. Therefore, the NPAC portal will leverage our comprehensive set of tools that form our identity and access management system.

To maintain maximum flexibility along with security, the portal will employ the model of an Account Administrator for each NPAC User company, with privileges to control user access in partnership with LNPA personnel. The Account Administrator will manage all user access within that company, specifying the various levels of authorization permitted by the portal, including:

- Which NPAC regions each user can access
- Which functions each user is permitted to perform, including:
  - Query-only

- Porting and pooling (i.e. Creates/Activates/Modifications/Disconnects)
- Request reports and BDDs
- Large project and SPID migration scheduling
- Access to NPAC billing and system monitoring data

The domains of the Account Administrators will be managed by LNPA personnel subject to the regional NPAC User Agreements as well as the various privileges assigned to types of users, i.e., SPs and providers of telecommunications-related services (PTRS). This model also will permit ancillary applications such as LEAP and the Intermodal Ported TN Identification service to be securely offered using the same framework—given that appropriate restrictions on data access will be maintained centrally based on a flexible user authorization model.

#### **NPAC Portal: Effective Industry Collaboration and Communication**

The resources managed by the LNPA are a critical reservoir of Industry expertise and experience, relied upon by Service Providers and lay-people alike—for everything from basic definitions of Local Number Portability to the schedules for upcoming SPID migrations. The LNPA also is a neutral common meeting ground for Service Providers across the Industry, to collaborate on common requirements and optimize cross-Service Provider activities. In recognition of this ongoing requirement, the NPAC portal will offer additional tools for knowledge-sharing and communication across the Industry.

To streamline communication between NPAC users, the Portal will allow for the online creation and maintenance of dedicated User Groups. These can act both as distribution lists for critical outbound notifications, and to control access to configurable user-managed “work-spaces”, within which the Portal can facilitate the exchange of ideas and information between a subset of NPAC Users. This can be particularly beneficial to the NPAC innovation and change management process, as a way to accelerate collaboration between SPs, vendors, and the LNPA.

#### **NPAC Portal: Access to Business Critical Information**

The NPAC Portal will allow access to critical information and processes, including:

- Real-time queries and audits of NPAC transactions
- Bulk-data downloads for SOA/LSMS audit
- Reports on:
  - NPAC data including SVs, network data, network objects, users, and profile setting
  - Inputs and outputs (file-upload, etc.)
  - Basic reporting functions (scheduling, formats)
  - Advanced analytics
  - Dashboards

### **NPAC Portal: Transition and Continuity**

Following Neustar's record of innovation with maximum continuity and backward compatibility for all NPAC Users, all transfers of functionality between existing interfaces and the NPAC portal will occur subsequent to comprehensive user documentation and training and without additional cost to the Industry.

### **RFP Required Enhancements**

The NPAC/SMS is constantly evolving and integrating new functionalities. Neustar and the Industry work together to define, approve, and implement new functionality on a regular basis. This section describes required new functionality that was asked about in RFP Section 7.

## **Security-Related Information**

### **RFP Required Enhancements: Support of IP Version 6**

Internet Protocol (IP) Version 6 is an evolution of the IP Version 4 that dominates the internet and communications networks today. It is important because it addresses the major concern that public IP addresses under version 4 are nearing exhaustion. Public addresses are expected to reach exhaustion in the United States in the next few years. IP Version 4 provides 32 bits for each address, while the newer IP version 6 provides 128 bits, allowing for many more unique addresses.

Neustar has anticipated this issue well in advance of its arrival. Neustar has been using IP Version 6 natively for over 6 years with commercial services, and is well-versed in IP Version 6 configuration, security, troubleshooting, and architecture. Most Neustar services have to be offered in both IP Version 4 and IP Version 6 worlds, which has its own unique set of challenges. Our teams of CMIP and networking experts have already started work on planning for the evolution of NPAC into the realm of IP Version 6. Neustar has led discussions on this topic in the LNPA Working Group forum, and we expect that group to approve of a solution and for Neustar to complete implementation by the end of 2014, well in advance of IP Version 4 address exhaustion.

The Neustar solution for IP Version 6 includes three important components:

1. **Network Engineering**—Neustar has already implemented IP Version 6 inside its own network. As part of the NPAC implementation, Neustar's networking experts will work with any Service Providers wishing to move to IP Version 6 to plan and coordinate the transition as it relates to NPAC connectivity.
2. **CMIP Application Changes**—the NPAC system conforms to RFC 1189 that defines the implementation of CMIP over TCP/IP. At the heart of the Neustar CMIP implementation is the Open Systems Interconnect (OSI) stack that provides CMIP functionality over TCP/IP. Neustar's CMIP protocol experts will integrate support for IP Version 6 into this OSI stack. Specifically, the IP Version 6 addresses are bigger in size than IP Version 4 addresses, and this will affect how the IP addresses are mapped to OSI addresses. As part of the implementation, Neustar's Operations Team will offer testing services to ensure that both Provider and NPAC systems are functioning properly end to end prior to production rollout.

3. **Other Interfaces**—Neustar is committed to supporting IP Version 6 connectivity to all of the interfaces to the NPAC. This includes the secure FTP site, the new NPAC UI, the new Security-Related Information, as well as any future interfaces.

Neustar views the transition to IP Version 6 as a slow evolution for the Industry. Consequently, all interfaces will remain backward compatible with IP Version 4. We expect that many Service Providers will decide to keep their NPAC related systems on IP Version 4 for many years to come. Neustar is well prepared for the transition as providers evolve their technologies.

**RFP Required Enhancements: Elimination of NPAC/SMS Support of Non-EDR**

Support for non-EDR functionality was eliminated under Statement of Work 86. The NPAC/SMS still must support some non-EDR features, such as the ability to respond to an NPAC user's query for an individual pooled number. Although not a part of the EDR functionality, Neustar remains prepared to provide an NPAC user with a Bulk Data Download (BDD) that includes individual number data for pooled numbers in cases where the NPAC customer is not yet able to process the now-standard EDR BDD.

From the NPAC/SMS customer's standpoint, the removal of non-EDR functionality is complete.

**Future Considerations**

This section describes required future considerations that were asked about in RFP Section 7.

**Future Considerations: Automation of processes between NPAC and PAS**

In collaboration with the Industry, Neustar will rely on its extensive experience as the LNPA and PA to further improve the interaction between the PAS and the NPAC/SMS.

Service Providers rely on accurate information from the PAS and the NPAC/SMS. Based on our experience as the LNPA and PA, we recommend automating the interaction between PAS and NPAC to allow requests from PAS to flow through to the NPAC/SMS. Once processed, the NPAC/SMS can interact with PAS to reflect an update in the status. We also propose the following additional improvements to the coordinating interface:

- **Automate change notifications from the NPAC to the PAS**—NPAC/SMS and PAS can communicate electronically to exchange information on pooling operations that need to be executed in the NPAC/SMS and automatically reflect said completion in PAS.
- **Automate validation of relevant fields in PAS**—Currently, validation is a manual process conducted by the NPAC Pooling Team. Automation will ensure that system checks are performed accurately and in a timely fashion and in keeping with the NPAC FRS while providing real-time and standard error codes for incorrect submissions.

Enabling real-time, automated communication between these two disparate and independent systems will improve overall data integrity and response time.

Neustar is the only vendor with the breadth of knowledge and experience in this domain to recognize the need for and offer solutions to seamlessly link both the NPAC and PAS systems, ensuring that both remain in sync, allowing for significant improvements in pool block provisioning activities for the entire industry.

#### **Future Considerations: Combining steps for Intra-Service Provider Ports**

New and expanded uses of the NPAC/SMS have evolved over the past several years, resulting in an increasing amount of information that can be stored in the NPAC database about a TN. It is common for SPs to perform an intra-SP port to provision data for NPAC records. The information about these numbers is established in the NPAC database and is disseminated to the Service Providers' LSMSs.

Because intra-SP porting volumes are likely to grow and intra-SP porting is less complicated than inter-SP porting. (e.g., Intra-SP porting does not require coordination between two different Service Providers), there has been interest in consolidating the Create Pending SV request with the Activate Pending SV request for intra-SP ports. There has been interest in also allowing the Service Provider's SOA to specify that the activation is to be delayed until a specified day and time.

In thinking about how best to accommodate the industry's interest in allowing Service Providers to consolidate and schedule intra-SP Create and Activate requests, Neustar considered the impact of large quantities of simultaneous delayed activations and whether it might be necessary to coordinate these intra-SP porting activities. We considered suggesting scheduling be done at the LNPA WG, but concluded a Service Provider initiating these intra-SP ports might not want to prematurely indicate its plans publicly. We also considered proposing transaction quotas, much like the approach used with SPID migration planning, but concluded this would be overly complex for the industry and difficult to administer. And we considered the use of the Mass Update/Mass Port (MUMP) process, since it would avoid publicly revealing the Service Provider's plans and would allow throttling should the quantity of simultaneously scheduled activations have an adverse impact on the LNP ecosystem. However, the industry's interest is in an improved approach for SOA initiation of intra-SP ports, not in further use of the MUMP processes.

Based on our over 15 years of experience working with the industry to develop NPAC/SMS functionality, we realized that the one-step SOA Create/Activate capability could be deployed without an artificial scheduling or quota system. This is because intra-SP ports driven by new or expanded uses of the NPAC/SMS should not require large quantities of simultaneous activations, unlike the case where transactions are performed for a network migration. The resulting design would avoid premature exposure of a Service Providers' network plans, allow a reduced Service Provider effort by eliminating the second SOA request message, require only minor changes to the NPAC/SMS platform, and introduce no backward compatibility issues.

Briefly described, the one-step feature would:

- Introduce a new attribute in the intra-SP Create Pending SV request
- Combine the Create and Activate requests to be performed as a single request
- Apply only to intra-SP ports
- Allow SOAs to include the new attribute on a per-request basis (i.e., no opt-in is required)

- Allow SOA to indicate NPAC/SMS should activate the pending SV
- Allow SOA to include a day and time in the new attribute to schedule delayed NPAC/SMS activation
- Provide for immediate NPAC/SMS activation if no day and time value is specified in the new attribute

Implementing a combined create and activate process for intra-SP transactions will greatly reduce the effort required by Service Providers to manage large jobs.

#### Future Considerations: Inter-carrier Communications

While the RFP referenced ICP only, we assume it intended to include LSR, therefore we will refer to this as ICP/LSR in this response. The NPAC/SMS architecture has the flexibility needed to incorporate the ICP/LSR processes that currently precede the NPAC/SMS LNP provisioning process. The existing NPAC/SMS architecture already has proven its flexibility by being able to support periodic changes required by the Industry. Examples include the introduction of Pooling, support of One Day Porting, pseudo-LRN, introduction of new optional fields, and the

Inclusion of ICP in the NPAC will require the expansion of the current NPAC Create and Modify messages utilized for porting between carriers. Existing messages can be expanded easily to include necessary data/fields for pre-port validation, E911, and Directory Assistance.

While the NPAC/SMS infrastructure can support and incorporate the functions performed today in the ICP/LSR process, NANC flows will require changes which in turn will introduce a number of complexities that will need to be worked by the Industry via the LNPA WG. One such complexity is the current use of a Clearinghouse/Service Bureau model. The NPAC/SMS can perform Clearinghouse/Service Bureau functions, but not without major changes to the NPAC/SMS. In addition the NPAC/SMS will need to create ICP/LSR business rules for wireline, wireless, intermodal, reseller, and carrier-specific scenarios. All this functionality will need to exist in the NPAC/SMS. Carriers should keep in mind that ICP/LSR in the NPAC will create transition costs as back-end system changes will be required to support new porting flows.

Wireless ICP can be assimilated into the NPAC/SMS process without difficulty. The <sup>Service-Related Information</sup> makes this change seamless as the addition of new fields to the schema can be published easily. However this requires major changes to carriers' back office systems and SOA systems as they will need to allow SOA/LTI entry, validation, and transmission of a WPR. Carriers also will need to support the validation, acceptance, and rejection of a port request based on a set of agreed upon data fields during the pre-port process.

In order to support Wireline and Intermodal porting (i.e., LSR), the Industry will need to address the standardization of the Wireless and Wireline porting process. Previous unsuccessful efforts at the LNPA WG to develop mapping between LSR/FOC data elements and Wireless/ICP data fields will require resolution to streamline the porting process and making it easy for the NPAC/SMS to support both Wireless and Wireline pre-port activities.

Other complexities are related to the support of non-bonded orders (orders submitted via a UI or fax). One solution can be the elimination of fax and e-mail support as we re-define porting flows. This will require small and medium size carriers to automate their SOA processes and use a mechanized interface into the NPAC/SMS or rely on service bureaus. This will help reduce the time it takes to port a number, but costs could outweigh benefits for small providers.

The bigger question is will ICP/LSR in the NPAC/SMS evolve in the future? How will this work in an environment dominated by mobile and IP services? ICP/LSR is likely to change considerably as communications evolve to mobile and IP. Just as mobile is simpler than wireline, it's likely that the process will continue to simplify as we move to IP.

A broader view should be taken when developing a solution. The Industry should avoid trying to fit the ICP/LSR process as it exists today into the NPAC/SMS. We see no benefit of taking on the complexities of the past, especially while those processes will apply to fewer consumers over time. There are systems and companies that support the current processes and they should continue to do so. However, as the newer, simpler processes are designed, it is these that should be integrated into the NPAC.

Neustar's suggestion is to open up the NANC flows and re-think the way porting is done today to accommodate open interfaces and the ability for carriers to authenticate port requests. This is an opportunity to simplify porting across the board and leverage existing NPAC/SMS functionality. A more comprehensive discussion is needed to ensure ICP/LSR in the NPAC/SMS is not simply taking existing ICP/LSR rules and standards and fitting them into the NPAC/SMS, but rather revamping and rewriting the NANC flows to accommodate future needs and porting in an all IP environment.

We believe that the work developed by the Out-of-the-Box subcommittee of the LNPA WG is an excellent start. The subcommittee was tasked with looking at streamlining existing process to accommodate the FCC's One Day Porting Mandate. Neustar believes this is the right framework to build out an architecture that supports ICP in the NPAC/SMS and address some of the complexities related to this effort.

#### Future Considerations: PSTN to IP Transition

The NPAC will be the most important tool Service Providers will use as the Industry transitions from the current TDM (time division multiplex) infrastructure to the future IP (Internet Protocol) infrastructure. The NPAC will be a critical component both during the transition and after. An authoritative method of mapping a TN to some type of Internet address (e.g., DNS name, URI, IP addresses) will be a requirement of the PSTN Transition. Thousands of Service Providers rely on the NPAC today for call and message processing for both TDM and IP networks. VoIP and text messaging have been around for many years and every provider that processes those calls and messages has relied on the NPAC for routing and administrative support. Not only does the NPAC provide the information necessary for these networks, it provides it in a manner that is familiar to companies that rely on advanced technologies for their day to day business operations. The NPAC is collaboratively managed by the Industry with a smooth change management process, it has a strong linkage to the authority of number administration, it has open APIs that process transactions in real time, and it is easily extensible to new features and functionality.

TNs have gone through three generations over the past century:

- **TN 1.0, TN is used as both a name and an address**—The first generation of TNs lasted for most of the 20th Century. In this generation the TN was used as both a name and an address. People used the TN as a name, i.e., “call this number to talk to me”. Networks used the same TN as an address—the first six digits, the CO code, identified the terminating switch. Networks used the CO code to determine how to route the call.
- **TN 2.0, Separation of the name and address**—In the 1990s the Industry implemented LRN (location routing number) technology which associates a dialed TN with a separate routing TN, an LRN which identifies the terminating switch. Networks used IN (Intelligent Network) technology to perform a query on the dialed TN to obtain the LRN. If there was an LRN, the network would use that to route the call. LRN enabled local number portability, number conservation via thousands block number pooling, and the ability for Service Providers to manage their networks in a more efficient manner. However it is important to note that the networks still use a CO Code for routing.
- **TN 3.0, Mapping of the TN to an Internet address**—When companies started implementing IP infrastructure in their networks they needed to map a TN to an Internet address because IP networks can't use TNs for routing. Right now this is mostly done by mapping the TN to the name of the Service Provider identified by the NPAC. The network then translates the Service Provider name into an Internet address that the networks can use to route the call. This process typically is referred to as ENUM. Not only is this process cumbersome—TN->SP->Internet address—it is typically done within a Service Provider's network, not between networks. That is, each Service Provider has to set up their own rules for the translation of TN->Internet address and that Internet address is only usable on that Service Provider's network. This has to change to enable Industry-wide IP interconnection.

### Mapping TNs to Internet Addresses

The creators of the Internet knew to separate the name from the address from the beginning; domain names resolve to IP addresses. Separation of name and address was implemented with TNs in the 1990s and this is a convention that must continue as TNs evolve to IP technology. There must be a method of mapping the TN to an Internet address.

However TNs have needs that domain names do not. TNs are a limited international resource, they are considered sensitive from both a competitive and a privacy perspective, they are tightly linked to emergency services, and TNs will be required to be used by Service Providers and consumers who have both TDM and IP infrastructure for some time.

### TNs are a Limited International Resource

Due to NAPM numbering conventions, there are 6.4 billion usable numbers in the North American Numbering Plan. However, because specific area codes are assigned to a state, exhaust of an area code occurs frequently, creating a great deal of work and disruption to consumers, Service Providers and regulators. The limited number of TNs requires that their utilization is closely scrutinized, and utilizations evaluated. This means the administrator must have the authority, skill, and experience to monitor, analyze and advise the Industry on use of the resource. Domain names on the other hand do not have the same concern. Second level domain names within a top level domain can have 63 characters and each character has 37 permutations, providing a virtually unlimited number of addresses. While there are about 100M names assigned in the .com domain, there are about 815M TNs assigned in the NANP.

#### **TN Administration Contains Sensitive Information**

Blocks of TNs are assigned to Service Providers which in turn assign TNs to either consumers or to resellers who then assign them to consumers. The fact that they are assigned to Service Providers for inventory provides some insight into their business. The Industry has implemented a Do Not Call database, for people who don't want calls from telemarketers, and the FCC has ruled that entities using auto dialers or recorded messages can't call mobile phones. The NPAC provides a list of wireline numbers ported to mobile service. The registry provider for TN to IP mapping must understand the sensitivities that the consumers, the Industry, and regulators have regarding information about numbering resources.

#### **TNs Will Coexist on TDM and IP Networks**

TDM nodes and networks will be around for some time. There have been suggestions that there should be a date, around 2018. TDM interconnect is no longer required by Service Providers. Presumably the TDM Service Providers would have to make arrangements for their traffic to be handled by an IP provider, which could map TN->Internet address. It's unclear if this will happen—it would require an FCC order—and if so, when it would happen. What is clear however is that the Industry is moving towards IP interconnection and a need to map TN->Internet address. And therefore it is clear that there will be an overlapping need to provide routing for both TDM and IP interconnects. The Industry does not want to duplicate the registry functionality existing in the TDM world with an entirely different registry provider for the IP world. In addition to being inefficient, it would also introduce the opportunity for conflicting data in the separate systems.

The Industry needs a TN->Internet address mapping solution that meets the needs of both TDM providers and IP providers for the foreseeable future. This system would need to support a real time interface for both, i.e., CMIP (current interface), and more web centric interfaces, i.e., web services interface (planned as part of NANC 372). The provider would need to understand all of the complex issues that are related to TNs such as conservation, competition, privacy, emergency services and the needs and capabilities of both TDM and IP providers.

The NPAC is the right tool and Neustar is the right provider to enable the transition of the PSTN from TDM to IP. The NPAC provides real time addressing information for both types of providers today. It is the state of the art for providing addressing data related to TNs. In addition, Neustar is an active Industry participant in all matters related to numbering. Not only are we the LNPA, we are also the NANPA and the PA. The Industry, Service Providers, vendors, regulators and others rely on Neustar as a source for numbering information and expertise. We are industry thought leader in the future of numbering. And we have the operational expertise to manage consensus and implement new processes and procedures related to numbering.

## Security-Related Information



Security Related Information



# Security-Related Information

# Security-Related Information



- **Incident management system**—pertinent information about events is recorded and managed as incident tickets. Neustar uses Service-Now as the primary incident management system for ticketing incidents managed by the Neustar NOC. Service-Now integrates with Netcool, the event management system to track the event from beginning to resolution.

### **NOC Monitoring Processes**

The NOC operates 24x7x365 and is managed by highly trained personnel who monitor and manage the NPAC infrastructure, triage production events via Security-Related Information , as well as other Network Management tools. Security-Related Information

Security-Related Information

# Security-Related Information

# Security-Related Information

## Security-Related Information



NOC processes are designed using proven methodologies derived from Information Technology Infrastructure Library (ITIL) foundations. ITIL is a set of practices, processes, procedures, tasks and checklists for IT service management. This streamlined and repeatable process ensures the proper response to an event. Automation of notifications provides the fastest method for addressing the event. Integration of the event management and incident management systems ensures the best possible documentation and mitigation of service affecting events.

### **Monitoring at Each Layer**

Neustar has established monitoring for all Layers of the NPAC/SMS architecture and NOC personnel quickly engage when appropriate.

### **Data Center Layer Monitoring**

Neustar strictly monitors and control access to the data center facilities 24x7x365. Security-Related Information

Security-Related Information



**Network Layer Monitoring**

The Network Layer is where Neustar customers connect to the NPAC/SMS. This Layer is designed to be highly available because of its critical nature and because Neustar coordinates with our customer's local IXCs.

Security-Related Information

In addition to utilizing SNMP agents and traps, the network engineering and operations teams also employ the following tools to monitor the network:



- Security-Related Information

- Security-Related Information

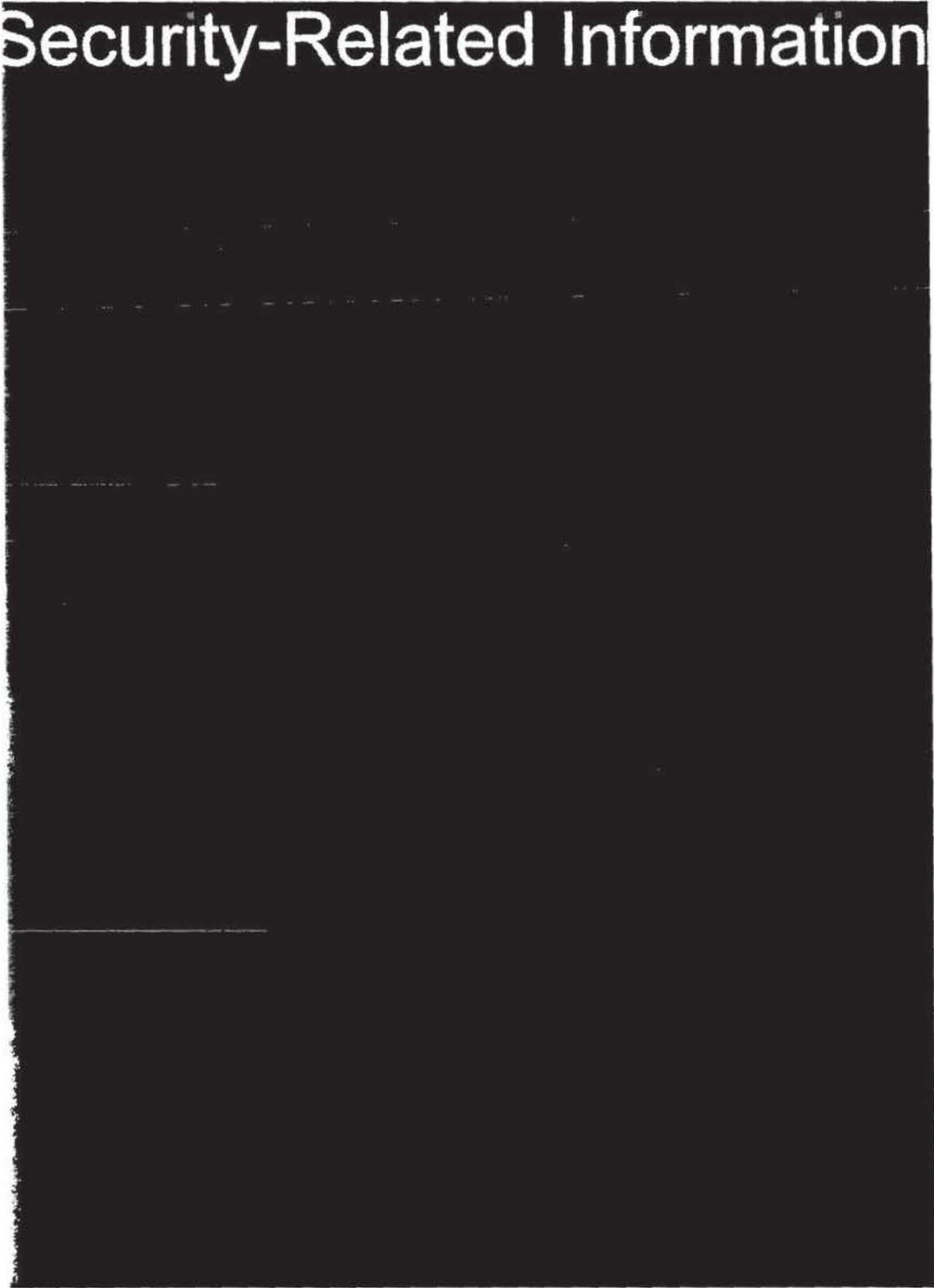
- Security-Related Information



The network operations team responds to all network alerts for the NPAC. The close collaboration between NOC and network operations allows for rapid response to events and the ability to predict problems before they occur.

# Security-Related Information

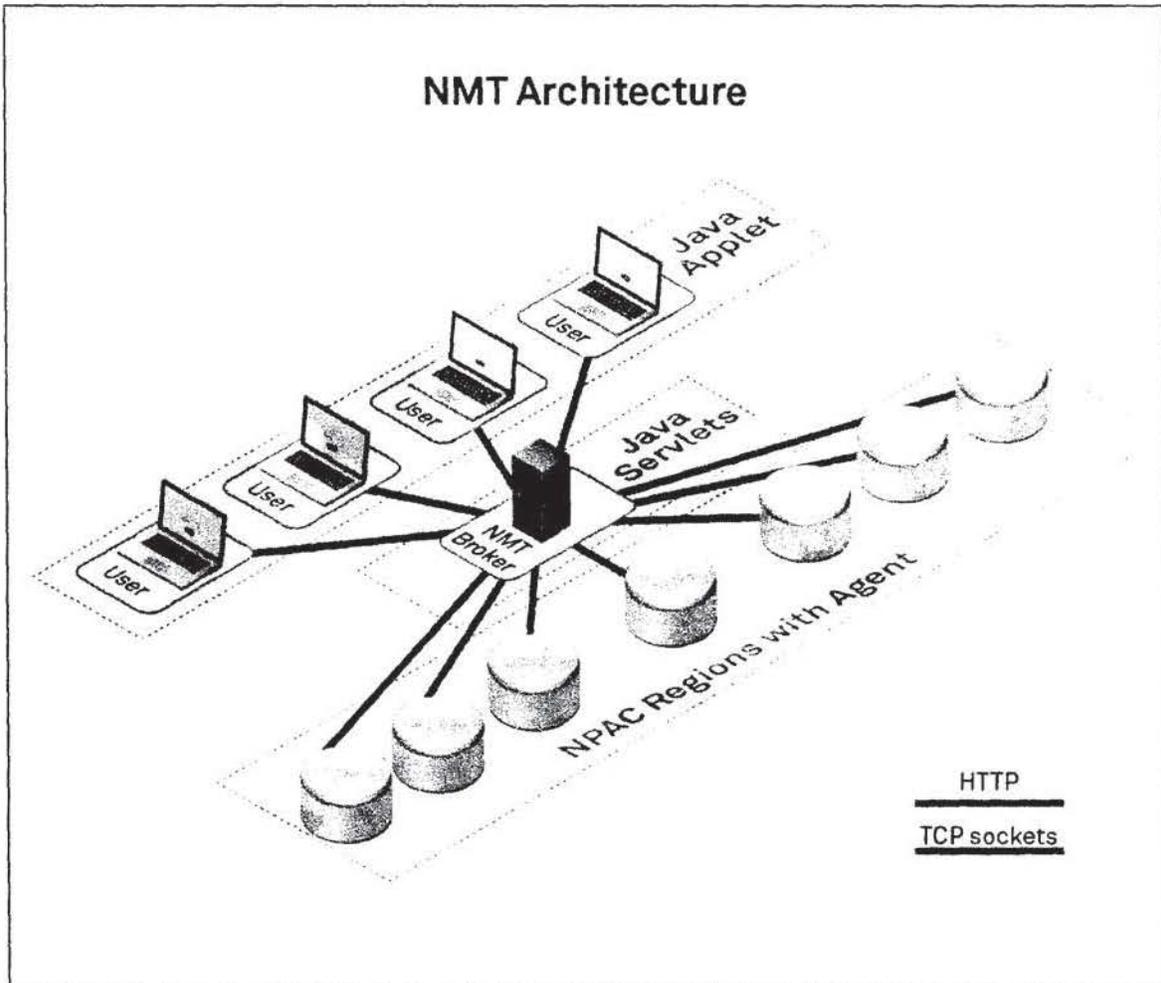
# Security-Related Information



# Security-Related Information



Security-Related Information



**Exhibit 1.2.3-6:** NMT provides an overview of all NPAC/SMS service-critical metrics.

As Mass Update Mass Port jobs are executed, the system tracks queues for LSMSs. If these queues rise above configurable thresholds, all jobs are suspended. This prevents failed LSMS broadcasts and ensures all LSMSs are synchronized. The system monitors the success rate of all work within each job. If a job has too many failures, it is paused so it can be reviewed and corrected. With both of these features, NPAC personnel are alerted whenever the system preempts a job.



Neustar has developed an extensive set of queries that analyze the production system for logical inconsistencies and that identify potential problems with Service Provider systems. For example, if an LSMS remains on the failed list of a subscription version for longer than one day then the subscription version is included in a report that is e-mailed to NPAC support personnel for investigation. This allows Neustar to remain in front of issues before they cause actual problems. Analysis of an issue is performed on copies of the production database to prevent interference with online processing.



Security-Related Information

# Security-Related Information

Security-Related Information

Neustar, the Neustar logo and "Real Intelligence. Better Decisions." are trademarks of Neustar, Inc.



## Security-Related Information

Security-Related Information



Security-Related Information

Security-Related Information

Security-Related Information



Security-Related Information

Security-Related Information

# Security-Related Information

## 1.3 Neustar's Approach to Operational Excellence

---



### Why Neustar

- Detailed methodology to release management including over 60,000 regression test cases
- Exceptional results from operations; audited by a third-party
- Investment in simulation of actual traffic patterns and characteristics to ensure high-quality software releases

### New for the Next Term

- Implementing and certifying in:
  - TL 9000 audit, which is designed for and by the communications Industry
  - ISO 27001 Information Security Standard, which minimizes and defends against security threats in the ever changing ecosystem
  - ISO 22301 Business Continuity Standard, which serves to further strengthen our ability to continue operations when faced with catastrophic events
- QA Testing and Release Management Processes
  - Software security assurance
  - NPAC User Interface load test to assess capacity and plan for future expansion of users
- Continuous integration to improve software code velocity

---

Operational excellence is often used to describe a company's total quality management (TQM) approach which usually includes at a minimum, measuring key processes, developing metrics and alerts, identifying anomalies or deviations from standard patterns, and driving continual improvement. Neustar's corporate-wide TQM includes those principles as well; however, we believe that most of our success is attributable to the following.

- Corporate and personnel-level **commitment to rigor, continuous improvement, and innovation via the consistent use of and adherence to industry best practices** in project management, software development and testing, change management, and service delivery while being agile enough to meet evolving needs.

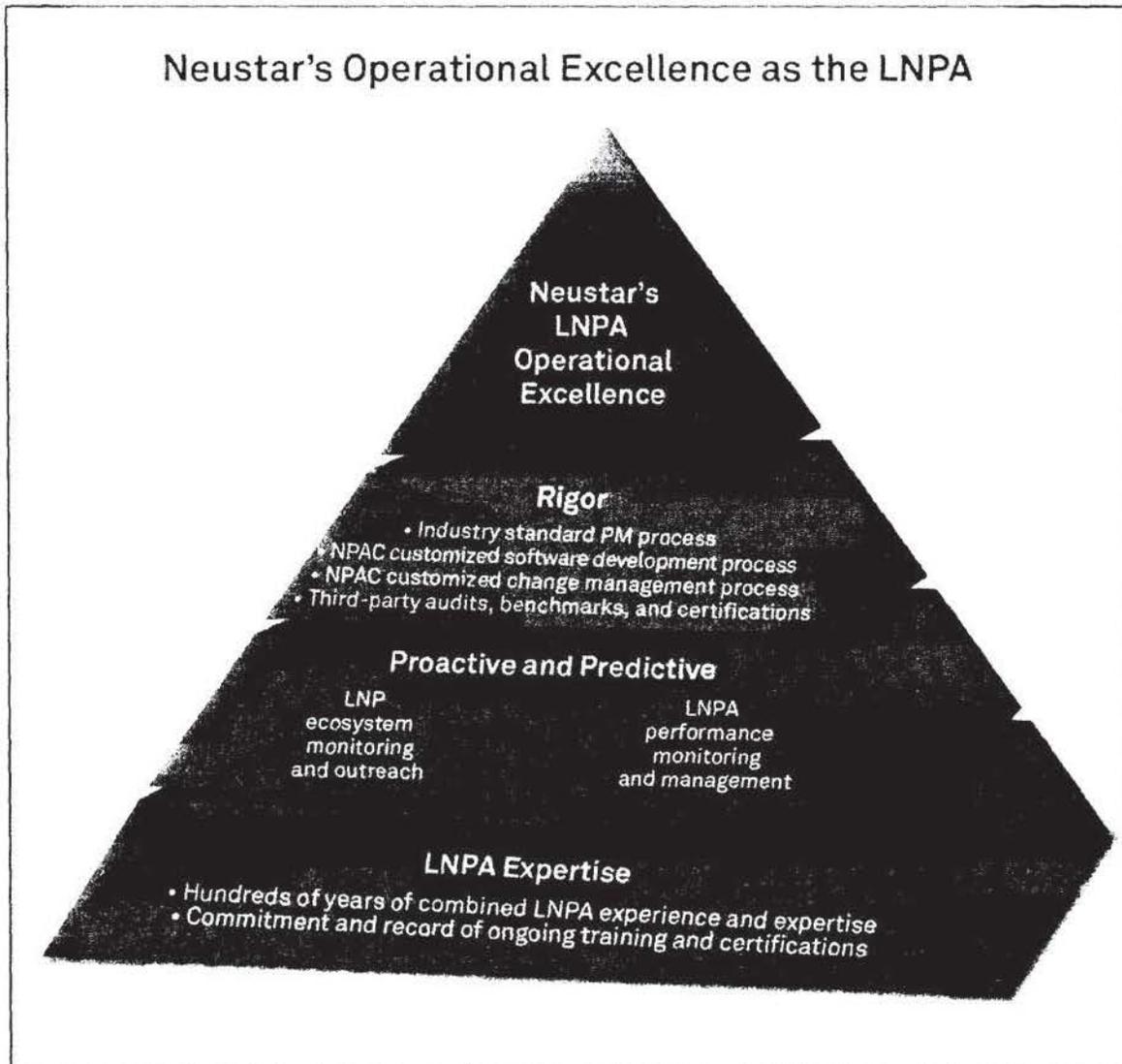
- Corporate and personnel-level commitment to the maintenance and satisfaction of various third-party audits, industry benchmarks, and certifications.
- **Proactive and holistic approach to performance monitoring and management** of not only the LNPA Service and system but also the LNP ecosystem, including Service Provider's LSMSs and SOAs, that could negatively impact NPAC/SMS performance and drive efficiency out of the system.
- **Leveraging subject matter expertise** and a corporate commitment to continually invest in human capital with training and certifications to ensure employee satisfaction. This expertise should be not only job specific (e.g., software development, security, etc.) but also expertise in Numbering, LNP, the NPAC/SMS, and the ecosystem the NPAC/SMS supports. Neustar's team of experts has been the single most important factor in our success as a vendor for the Industry—not just for LNPA but also for other Industry-wide services like Thousands-block Number Pooling Administration and NANP Administration. Our personnel are active in many forums that seek to develop and implement policies that address the changing needs of the Industry—for example, PSTN to IP migration, IP interconnection etc. We describe our LNP expertise further in Proposal Section 2.4, LNP Expertise.

Each element highlighted above, depicted in Exhibit 1.3-1, and described in further detail below, has enabled us to continually improve over the years to deliver reliable, predictable levels of performance thus allowing Service Providers to focus their resources and attention on revenue-generating objectives rather than expend energy to manage a poorly performing vendor.

### 1.3.1 Rigor Through Consistent Use of and Adherence to Industry Best Practices

#### Neustar's Project Management Approach

The old adage rings true: failing to plan is planning to fail, particularly when implementing changes to an Industry-wide infrastructure resource such as the NPAC/SMS where every SP must continue to be able to operate and affect portability seamlessly. Developing and implementing a solid, realistic plan requires both function-specific expertise and experience (e.g., certified project managers) and subject matter expertise and experience (e.g., experience implementing NPAC/SMS changes). Without this, the LNP Administrator cannot develop a plan that adequately addresses the requisite activities/milestones, the resources required, dependencies, or the duration of these activities, including any environment considerations (e.g., Industry needs regarding testing times, documentation requirements, training requirements, etc.). Neustar understands this and has invested in two corporate-wide project management organizations (PMO)—one for NPAC Infrastructure and Operations and one for NPAC Software Development and Testing—which are responsible for overall coordination of every change to the NPAC/SMS from the standard, routine maintenance-type changes up to major software release and technology refresh projects to ensure every change made to the NPAC/SMS is well managed, leverages the appropriate expertise and resources, and is governed by a set of documented, proven project management processes and methodologies.



**Exhibit 1.3-1:** Neustar leverages unmatched expertise to take a proactive approach to managing with rigor to deliver predictable and reliable services to the Industry.

Our PMBOK-based approach to project management for NPAC projects will continue to encompass the management of the following critical components:

- Project schedule
- Staffing
- Project organization
- Monitoring and control

- Risk management
- Project planning and tracking
- Communication
- Issue escalation
- Quality assurance (QA) monitoring

### Neustar's Software Development Process

Neustar follows custom ISO 9001:2000 certified processes finely tuned from years of experience managing the NPAC to ensure successful production rollout that does not impact the LNP ecosystem or NPAC/SMS performance. Our NPAC Development team works closely with the NPAC QA and Operations teams from start to finish ensuring all teams are fully aware of the operational implications of the implementations provided by NPAC Development. This collaboration takes the form of joint planning sessions where the teams discuss the proposed feature/change and make joint decisions on high-level requirements, as well as transition meetings held prior to delivery.

TMNG assesses Neustar's Software Release Management process to be well above what is typically encountered in the industry.

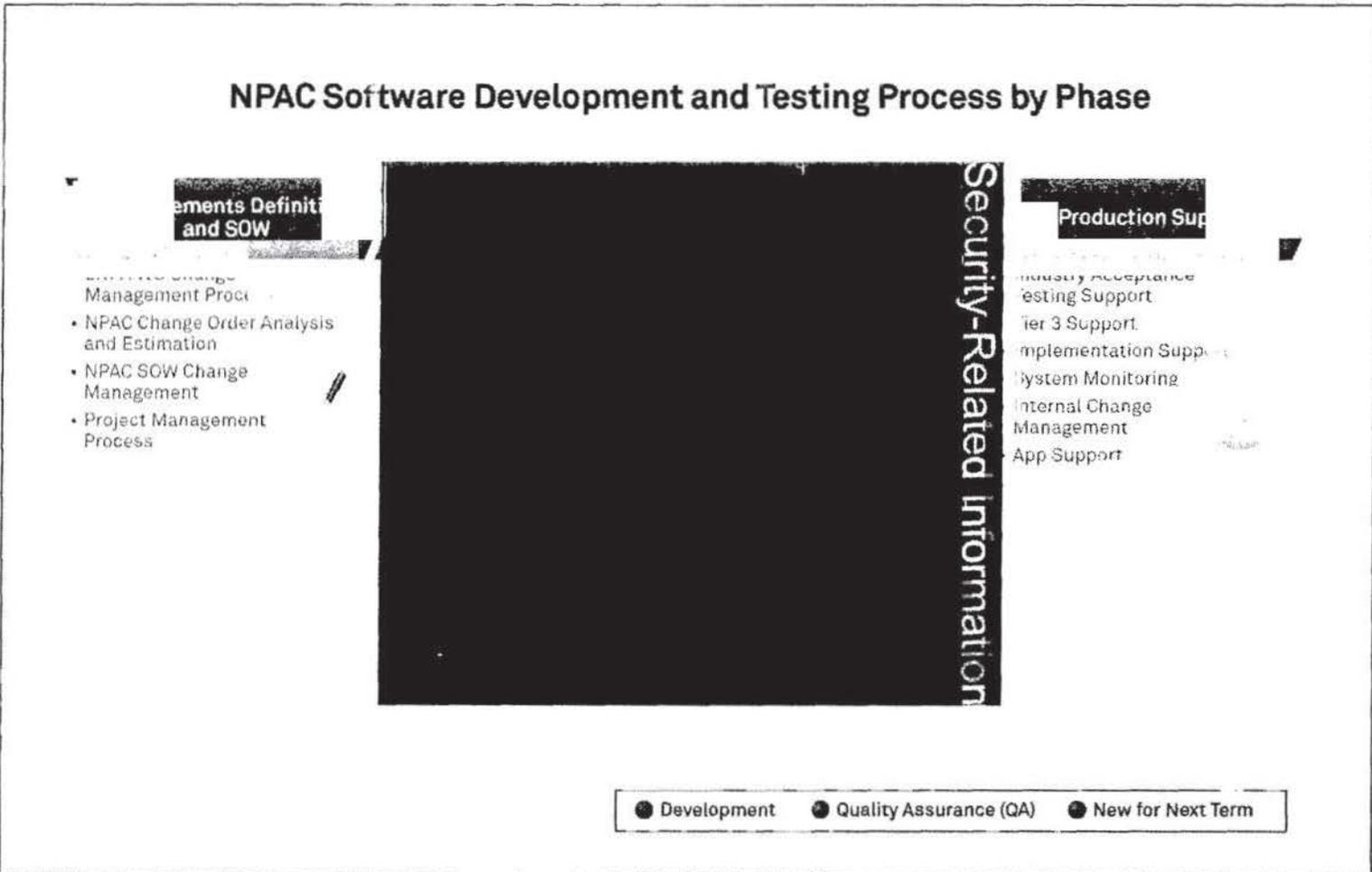
TMNG—2012 Article 14 audit

The following is a high-level outline of the Customized NPAC Software Development and Testing Process and is shown in Exhibit 1.3-2.

#### Requirements Definition and Statement of Work (SOW)

The NPAC Development process provides input and support to the NPAC SOW Development Process as described below. This phase is iterative in nature and comprises a two-way process. Neustar, as the LNPA, proposes requirements (driven by continuous improvement and refinement objectives) to the Industry and receives and processes feedback:

- **LNPA-WG Change Management**—Neustar's NPAC representatives participate in LNPA WG meetings as NPAC change order requirements are discussed, refined, prioritized, and documented. Our development team reviews and analyzes the requirements to ensure they are clearly defined, technically feasible, and can be implemented within the requested timeframe.
- **NPAC Change Order Analysis and Estimation**—Neustar gathers up technical inputs from various internal teams to draft the SOW. We analyze the NPAC release package to resolve issues, answer questions, verify the scope has not changed, assess impacts to the current NPAC/SMS, prepare level-of-effort estimates, and create draft schedules. This process may occur multiple times until a final, negotiated release package is approved by the NAPM LLC and Neustar.
- **NPAC SOW Change Management**—Neustar's Customer Relations team notifies NPAC Development/QA that the NPAC SOW is approved and development of the new release begins. The negotiated release package, including the approved change orders, is used throughout design and development.



**Exhibit 1.3-2:** Neustar's unique approach to NPAC SW development enables us to consistently perform over 25 iterations of testing cycles, running over 60,000 test cases, and deliver near-perfect application releases to production.





## The Neustar Difference

While there are very strong parallels between Neustar's custom approach to NPAC Software Development and the Agile Manifesto, our approach is customized for the NPAC/SMS and has proven to be very successful. The advantages of this tight integration between our Development and QA teams include:

- The ability to absorb any last minute changes with the sense of confidence that comes with executing Automated Testing—even for the new features in the release—no matter how late these changes are decided. Manual testing cannot achieve this level of confidence due to time pressures.
- Software quality is an evolutionary process where software gets better after each iteration. Using fully automated testing enables many more iterations of internal releases and test cycles than can be achieved by segregated/out-of-synch software teams. Security-Related Information
- The QA/Dev Team's early access to internal builds enables early detection of issues, allowing ample time for reliable fixes. In addition, early access reduces the amount of testing that the QA/Dev Team has to do, allowing us to move faster and focus on more sophisticated development problems.
- Security-Related Information

### QA Testing and Release Management

Prior to the Integration Test phase, the NPAC Development Release Control Board (RCB) meets to review the status of NPAC code, decide on which defect fixes and enhancements to include in the release, and determine the most appropriate release type (e.g., major, point, patch). In addition, the NPAC Development Systems Architect prepares Release Notes that describe (for Applications Support) the release contents, any known issues included in the release (if applicable), and installation and back-out instructions as required. 'Known issues' are also documented in the Security-Related Information system for RCB consideration in a future release.

### Security-Related Information

Neustar has studied the traffic patterns on Production Regions very closely over the years, and developed Load Generators that simulate predicted production load volumes. This helps with future capacity planning and flawless operations under spikes of volumes, whether it's network maintenance or launch of new phones by a Service Provider.

For the next term, we plan on implementing the following refinements:



- **Security-Related Information**
  
- **GUI Load Test to assess capacity and plan for future expansion of users**—As more features are made available to SPIDs, the use of NPAC GUI is increasing. We will use **Security-Related Information** to develop load and performance tests to measure how fast it is expected to perform under real-life transaction volumes and measure the capacity of NPAC UI. By using this, we strengthen our ability to accurately anticipate future capacity needs.
- **Break Testing to assess and improve system's reliability even further**—Developing a set of catastrophe scenarios, for example, killing processes in the middle of transactions, to assess the resilience of the NPAC system. Such testing would tell us potential data/transaction loss during unexpected catastrophic events, so that we prepare even better for such disastrous scenarios.
- **Continuous Integration to improve code velocity**—Implementing a daily task that kicks off the build process automatically, integrating pieces each engineer is working on, and deploy the build on all Dev and QA servers. Continuous Integration allows integrating pieces more often and in smaller chunks so we can resolve integration problems faster. This would be followed by kicking-off a set of Automated Sanity Tests to test the build allowing Development Engineers to make use of Automated Tests during their integration.

## The Neustar Difference

During this phase, there are several things that Neustar does that sets us apart from our competitors. These include:



- **Security-Related Information**

- **Meticulous internal acceptance testing.** For example, when making a major change that involves data conversion, the NPAC Applications Team receives a copy of the production data and runs through the actual upgrade on each region to make sure we don't encounter data-specific issues that could never be found in the QA environment due to the nature of the data. The added benefit of this exercise is that it gives the NPAC/SMS Application Team the opportunity to rehearse the procedures such that at deployment time they are just repeating steps they have executed successfully already.

The following functions are aligned in support of these phases:

- **Tier 3 Support**—NPAC developers assigned to Tier 3 Support investigate and verify a defect, evaluate the impact severity, open a ticket and maintain information about the problem in ALM, and determine the appropriate course of action. Potential actions include 1) identify a work-around solution and schedule fix for a future point release, 2) build an emergency patch release containing a code fix, and 3) provide an explanation for the system behavior. Tier 3 Support is available 24x7x365.
- **Project Management (PM)**—NPAC Software PMO is responsible for planning, coordinating, and oversight including task estimation, project scheduling, resource management, risk management, project cost and budget tracking, and project close-out. In addition, the NPAC Director, CMA, and NPAC Project Manager plan the manpower, training, hardware, facilities, and other resources needed to complete the project. The project schedule and cost estimates are updated at the end of system design and detailed design to factor in revised work-hour estimates and actual hours worked.
- **Configuration Management (CM)**—The CM Engineer manages the build and release process used for Integration, System, and Patch Release testing. This includes generating builds, installing builds on development boxes, releasing source code and contacting developers to resolve issues when builds fail. The System Architect is responsible for writing release notes, coordinating and conducting release readiness reviews with the assistance of the Project manager, moving approved releases, and supporting release notes to an FTP site for use by Application Support in their verification, validation, and Production implementation. In addition, the System Architect implements and maintains CM standards and procedures, reviews technical product specifications to ensure overall product quality, maintains CM documentation, and creates release packages and release notes. Records of all releases can be found in the Telelogic CM Synergy repository.

#### Security-Related Information

## The Neustar Difference

In conclusion, typical software development programs have testing in place but not every vendor undertakes testing with the same approach and vigor. Security-Related Information



As the current NPAC provider, Neustar has successfully implemented 11 major software releases to the NPAC system, each one in conformance with new requirements, provided on time and within budget, and with Security-Related Information

Exhibit 1.3-3 provides a listing of third-party audits and shows how we have improved over the past years in Software Release Management.

Neustar is ISO 9001:2000 certified for the NPAC system. Detailed region roll-out plans are developed and executed for the implementation of NPAC/SMS software releases in the production NPAC regions. Exhibit 1.3-4 is provided for reference as a sample of a region rollout plan.

### Security-Related Information

This may not be intuitive to a less experienced vendor that might not appreciate the consequences of introducing errors. Problems that surface during implementation in production can take on a life of their own and very quickly overwhelm not just the NPAC but the entire ecosystem and can even cause carriers to lose their ability to transact with the NPAC. Security-Related Information

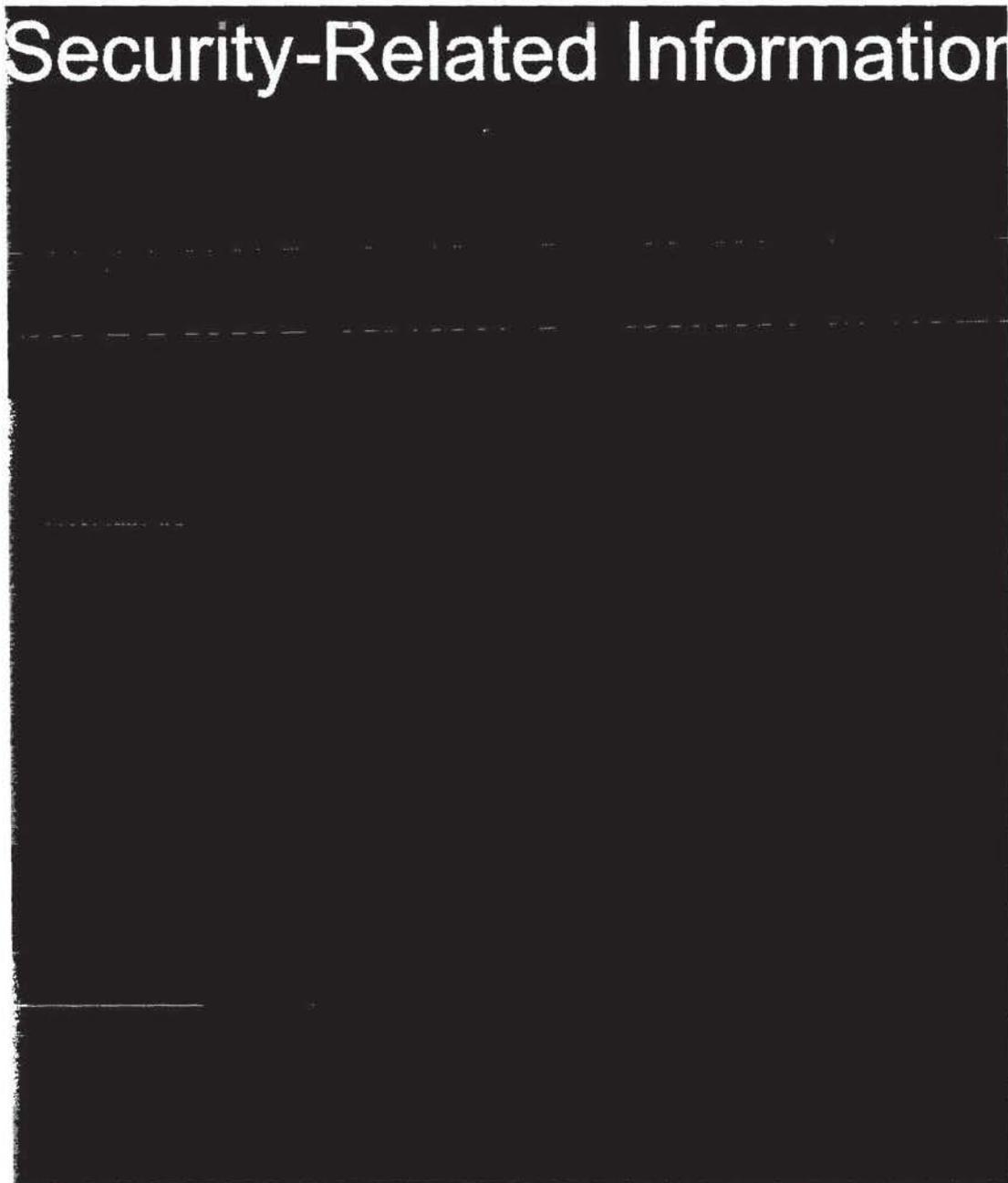
### Software Release Management—Article 14 Audit Scores

Category	2008	2012	Trend
<b>Software Release Management Overall Score</b>	4.50	4.66	▲
<b>Protecting Service Providers Operations</b>	4.50	4.67	▲
<i>Certification and Regression Testing</i>	4.40	4.67	▲
<i>Interoperability Testing</i>	5.00	5.00	→
<i>Software Defect Management</i>			▲
<b>Delivering New Software Releases</b>			
<i>Complete Release Life Cycle</i>	4.50	4.59	▲
<i>Requirements Analysis &amp; System Design</i>	5.00	5.00	→
<i>Development</i>	4.10	4.20	▲
<i>Neustar Quality Assurance</i>	5.00	5.00	→
<i>Industry Testing Support</i>	4.50	4.60	▲
<i>Production Rollout and Rollback</i>	4.30	4.50	▲
<i>Project Management</i>	4.40	4.40	→
<b>Maintaining Release Management Support</b>	4.30	4.36	▲
<i>Business &amp; System Expertise</i>	4.10	4.20	▲
<i>Trained Staff</i>	4.10	4.20	▲
<i>System Architecture</i>	4.50	4.50	→
<i>System Documentation</i>	4.50	4.50	→
<i>Infrastructure and Support Tools</i>	4.50	4.50	↔

- 5 - Excellent performance, far exceeds industry best practices
- 4 - Above average performance, generally exceeds industry best practices
- 3 - Average performance, meets industry best practices
- 2 - Below average performance, fails to meet industry best practices
- 1 - Poor performance, falls far below industry best practices

**Exhibit 1.3-3:** Third-party audits validate our performance and provide valuable input on possible future enhancements.

# Security-Related Information



### Neustar's Internal Change Management Process

Waiting for system components to fail or come to "end of life" is not a responsible strategy for ensuring carrier-grade performance. Once changes are deemed necessary, we follow an ISO-certified, NPAC-customized Change Management process (shown in Exhibit 1.3-5) to virtually eliminate risk and maximize success. The following are highlights of Neustar's approach that we will continue to use in the next term:

- Security-Related Information
- Neustar Infrastructure & Operations Teams perform proactive maintenance on the NPAC/SMS to ensure optimal performance. Examples include, database index rebuilds, storage array quarterly health checks, chassis hardware firmware upgrades, hardware server reboots, operating system upgrades, network upgrades, and security firewall upgrades. Security-Related Information
- Standardized and documented Change Requests are reviewed and approved by NPAC Product, Customer, and Technical Management teams at a weekly Change Management Advisory Board Meeting.
- Neustar's Operations Team develops a Rollout Plan detailing the software application implementation steps and timeline for implementing NPAC/SMS software application releases in the NPAC Customer Test Environment (CTE) and Production Regions. Neustar performs comprehensive Acceptance and Region Readiness Testing, and coordinates and executes Industry certification Turn-up Testing with Service Providers and their vendors for software application releases prior implementing Production.

### The Neustar Difference

Applying lessons learned throughout our tenure, Neustar has refined the CM process to introduce safeguards designed to execute releases and changes more seamlessly to the Industry. Security-Related Information



# Security-Related Information



# Security-Related Information

Further, we use a customer-mirrored, internal production system for a few weeks prior to deploying to the customer facing production system. Whenever possible, we install the change in just one region for a “burn-in” time of two weeks and actively monitor any new component for anomalies to ensure there are no unwanted side effects or issues internally, or impacts on external systems—SOAs, LSMSs, and NPAC UI users. If there are problems identified, they are addressed quickly, thus minimizing their impact. If the burn-in period has elapsed with no problems, we deploy the change into the remaining regions over several industry-defined maintenance windows. This approach has helped us eliminate virtually all risk to customer systems and NPAC performance.

### 1.3.2 Rigor Through Third-party Audits, Benchmarks, and Certifications

Audits and Benchmarks are an essential part of Operational Excellence. Neutral independent auditors allow Neustar, the NAPM, NPAC Users, and the FCC to see empirical data that Neustar, as the LNPA, is meeting and/or exceeding all obligations—service delivery, system performance, and contractual. Further, given the evolving nature of these audits, they provide valuable insights with recommendations to enable Neustar to design and implement solutions to improve operations. The following tables (see 1.3-1, 1.3-2 below) highlight the various third-party audits to which we are subject as part of our LNP Administration contract; our record of superior performance under those audits; and the certifications we have in place and are proposing for the next term to ensure we continue to meet the needs of the Industry going forward.

In addition to the many yearly audits and benchmarks already performed, we are proposing adding several new audits for the next generation NPAC operations to continue to improve overall operations via the TL 9000 audit (specific to telecom vendors), as well as ISO 27001 “Information Security” and ISO 22301 “Business Continuance” audits.



### The Neustar Difference

Supporting these audits isn’t an exercise of simply checking the box to be contractually compliant. Neustar has found that there is real value in these audits. We also established effective relationships with the Industry representatives based on mutual respect and a commitment to use these audits and findings as a powerful tool to continue to improve the overall service we deliver and the systems and tools we use. This has significantly strengthened our approach and ability to deliver service.



Table 1.3-1. NPAC Audit Overview

Audit / RFP Section	Value
	<b>100% compliance over the last 5 years</b>
Gateway Evaluation Process “GEP” (RFP Section 4.1)	<ul style="list-style-type: none"> <li>• Focuses the LNPA to deliver excellence in system performance and vital administrative activities.</li> <li>• Validates the LNPA’s performance via a neutral third-party auditor</li> <li>• Foundation block of “Operational Excellence”</li> </ul>
	<b>100% compliance since inception in 2003</b>
Neutrality Review (RFP Section 4.2)	<ul style="list-style-type: none"> <li>• Provides “factual judgments” and “legal opinions” on Neustar’s compliance with the Neutrality Code of Conduct, and other matters, from a neutral third party</li> <li>• Validates LNPA remains impartial and is not aligned with any particular</li> </ul>

Audit / RFP Section	Value
	<ul style="list-style-type: none"> <li>telecommunications industry segment.</li> <li>Performed by a neutral, third-party auditor.</li> <li>Validates access to the NPAC/SMS for all qualified Users is at all times evenhanded, impartial and nondiscriminatory.</li> <li>Validates the entity is not subject to undue influence</li> <li>Validates the LNPA's (and any sub-contractor's) adherence to a Neutrality Code of Conduct.</li> </ul>
<p>NPAC/SMS Data Center Operations Audit (RFP Section 4.4)</p>	<p><b>Above Average / Best in Class over the last 5 years</b></p> <ul style="list-style-type: none"> <li>Validates the LNPA's Data Center operations against industry best practices.</li> <li>Performed by a neutral, third-party auditor.</li> <li>Ensures the LNPA's Data Center operations continually keep up with evolving standards.</li> <li>Foundation block of "Operational Excellence"</li> </ul>
<p>Benchmarking Process (RFP Section 4.6)</p>	<p><b>100% compliance over the last 5 years</b></p> <ul style="list-style-type: none"> <li>Allows the Customer to select a targeted benchmark of operations that is deeper than other contractual audits.</li> <li>Validates the LNPA's operations against industry best practices.</li> <li>Performed by a neutral, third-party auditor.</li> <li>Ensures the LNPA's operational activities align with evolving standards.</li> <li>Foundation block of "Operational Excellence"</li> </ul>
<p>New User Evaluator (NUE) Process (RFP Section 5.1)</p>	<p><b>100% compliance since inception in 2009</b></p> <ul style="list-style-type: none"> <li>Neutral, third-party auditor reviews every use of User Data by Neustar's User Services, all other providers of telecommunications-related services are reviewed only for their initial proposed use of User Data.</li> <li>Neutral, third-party auditor determines whether access to NPAC is necessary and intended use is a Permitted Use.</li> <li>Neutral, third-party auditor ensures Neustar, in its activities as a User, is not advantaged because it is also the LNPA</li> </ul>
<p>Intermodal Ported Telephone Number Identification Service (RFP Section 11.1)</p>	<p><b>100% compliance since inception in 2004</b></p> <ul style="list-style-type: none"> <li>Neutral, third-party auditors conduct neutrality, performance, and cost reviews.</li> </ul>
<p>LNP Enhanced Analytical Platform for Law Enforcement Agencies and Public Safety Answering Point Providers (RFP section 11.2)</p>	<p><b>100% compliance since inception in 2006</b></p> <ul style="list-style-type: none"> <li>Neutral, third-party auditors conduct neutrality, performance, and cost reviews.</li> </ul>

**Table 1.3-2. NPAC Industry Certifications Overview**

Industry Certification	Value
ISO 9001:2000 Quality Management System	<p><b>Results from 2008-2012</b></p> <p>Security-Related Information</p> <ul style="list-style-type: none"> <li>Validates the LNPA's performance via a neutral, third-party auditor</li> </ul>
Sarbanes Oxley	<p><b>Results from 2008-2012</b></p> <p>0 Material Weaknesses; 0 Significant Deficiencies</p> <ul style="list-style-type: none"> <li>Validates the LNPA's performance via a neutral, third-party auditor.</li> </ul>
TL 9000 Quality Management System Replaces ISO 9001	<p>New for the next term:</p> <ul style="list-style-type: none"> <li>Built on ISO 9001's eight quality principles and is designed specifically for the communications industry by the communications industry.</li> <li>Defines unique communications quality system requirements for design, development, production, delivery, and service.</li> <li>Specifies measurements for companies to help evaluate effectiveness of quality implementation and improvement programs.</li> <li>Validates the LNPA's performance via a neutral, third-party auditor.</li> </ul>
ISO 27001 – Information Security	<p>New for the next term:</p> <ul style="list-style-type: none"> <li>Systematically examines the organization's information security risks, taking account of the threats, vulnerabilities, and impacts.</li> <li>Includes a coherent and comprehensive suite of information security controls and/or other forms of risk treatment (such as risk avoidance or risk transfer) to be implemented to address risks deemed unacceptable.</li> <li>Adopts an overarching management process to ensure information security controls continue to meet the organization's information security needs on an ongoing basis.</li> <li>Validates the LNPA's performance via a neutral, third-party auditor.</li> </ul>
ISO 22301 – Business Continuity	<p>New for the next term:</p> <ul style="list-style-type: none"> <li>Sets the standard for program development, and supporting policies, guidelines, and procedures needed to ensure a firm's business continuity regardless of adverse circumstances or events.</li> <li>Validates the LNPA's performance via a neutral third party auditor.</li> </ul>



### 1.3.3 Performance Monitoring, Reporting, and Management for the NPAC/SMS and the LNP Ecosystem

Given the complexity of the service and system delivery, there are several large organizations within Neustar focused on our success. In order to ensure these organizations are working in lockstep towards overall operational excellence, we created a function solely responsible for the overall, holistic view of NPAC Operations and Performance. This team works with various NPAC teams (e.g., Operations, Technical Operations, Software Development, Security, Customer Relations, Product Management, etc.) to monitor, collect, review, report on, and proactively provide risk assessments and risk mitigation strategies for all activities surrounding the NPAC including real-time throughput, performance and trending metrics, labor, technology, major projects, and customer support activities which include provisioning, performance, and stability of the entire LNP ecosystem, as well as audits and benchmarks.

The team reviews in detail all NPAC metrics including the SLRs (see Table 1.3-3 below), audit results, labor, and key milestones during regular meetings scheduled with the Senior Vice Presidents of Infrastructure and Operations (I&O) and SW Development. Monthly meetings are held with the CEO, CFO, and SVPs of Human Resources and I&O to review all aspects of the NPAC service and prioritize activities. This ensures all parties have a common understanding of NPAC performance and activities and allows for open discussions of any concerns or issues to address the same before they become larger, more complex issues.

Table 1.3-3. SLR Overview

New SLR	Description	RFP Requirements	Performance / Plans for 2015-2022
1	Service Availability	99.99% Availability —increased from 99.9%	Greater than 99.99% availability in 2012 <i>New for 2015:</i> Introducing additional local and site-failover automation to restore service quickly and without disruption for Service Providers
2	Scheduled Service Unavailability	As Agreed by Parties	All SLRs met in 2012
3	Partial Service Unavailability	10 minutes to restore service— <i>new SLR</i>	See SLR 1; local and site-failover automation supports SLR 3 as well
4	LSMS Broadcast Time	3 second average response time— <i>decreased from less than 60 seconds</i>	Average 30 millisecond response time in 2012
5	SOA to NPAC Interface Rates	99.9% of transactions maintain a min of 7 CMIP tps— <i>increased from 95%</i>	Average above 99.9% in 2012 <i>New for 2015:</i> Introducing additional application layer optimization to accommodate increased throughput
6	NPAC to LSMS Interface Rates	99.9% of transactions maintain a min of 7 CMIP tps— <i>increased from 95%</i>	Average above 99.9% in 2012 <i>New for 2015:</i> Introducing additional application layer optimization to accommodate increased throughput
7	SOA-LSMS Interface Availability	99.99% Availability— <i>increased from 99.9%</i>	100% availability in 2012 <i>New for 2015:</i> Ethernet connectivity

New SLR	Description	RFP Requirements	Performance / Plans for 2015-2022
			options available to support increased redundancy and bandwidth
8	Unscheduled Backup Cutover Time	Maximum of 10 minutes to cutover to the backup site	All SLRs met in 2012
9	Partial Disaster Restoral Interval	Equal to or less than 4 hrs — <b>decreased from 24 hours</b>	All SLRs met in 2012
10	Full Disaster Restoral Interval	Equal to or less than 6 hrs — <b>decreased from 48 hours</b>	All SLRs met in 2012
11	Administration of Any NPAC/SMS Table	99.99% error free— <b>increased from 99.5%</b>	All SLRs met in 2012
12	User Problem Resolution, Average Speed of Answer	Minimum of 90% of calls answered by live operator within 10 secs (during normal business hours)	Average over 99% calls answered within 10 seconds in 2012
13	User Problem Resolution, Abandoned Call Rate	Less than 1%abandoned call rate— <b>decreased from 2%</b>	.1% Abandoned call rate in 2012
14	User Problem Resolution, After Hours Callbacks	99% callback within 15 minutes (outside normal business hours)— <b>decreased from 30 minutes</b>	Two SLRs missed in 2012, due to failure of after-hours voice mail system (replaced 3Q 2012) <i>New for 2015:</i> Migration to 24x7 Help Desk
15	User Problem Resolution, Commitments Met	100% commitment to get back to User— <b>increased from 99.5%</b>	100% compliance in 2012
16	Logon Administration	99.5% of all approved request within 6 hrs of receipt— <b>changed from 12hrs and increased from 99%</b>	100% compliance in 2012
17	Unauthorized System Access - Security Error Log	Monitor and record unauthorized access	All SLRs met in 2012
18	System Security Remedy Invalid Access Event	Remedy logon security permission errors immediately after user notification	All SLRs met in 2012
19	NPA Split/Mass Changes	Notify User within 10 days business days of receipt of notification of the need for NPA Split/Mass Change	All SLRs met in 2012
20	Unscheduled Service	Notify User within 15 minutes of detection	All SLRs met in 2012

New SLR	Description	RFP Requirements	Performance / Plans for 2015-2022
	Unavailability Notification — Upon Detection		
21	Unscheduled Service Unavailability Notification — Update	Provide 30-minute updates	All SLRs met in 2012

Security-Related Information



- Security-Related Information

**Conclusion**

Neustar’s Operational Excellence (OpEx™) program, which combines rigor, commitment, industry best practices, and unmatched expertise in LNP Administration, has produced extraordinary results over the past five years and will ensure the highest levels of quality at the least risk, for the next term. If selected as the next LNPA, we will continue to demonstrate this same level of expertise and commitment to Operational Excellence. Exhibit 1.3-7 shows the impact that our Operational Excellence program has had on our image as a partner.

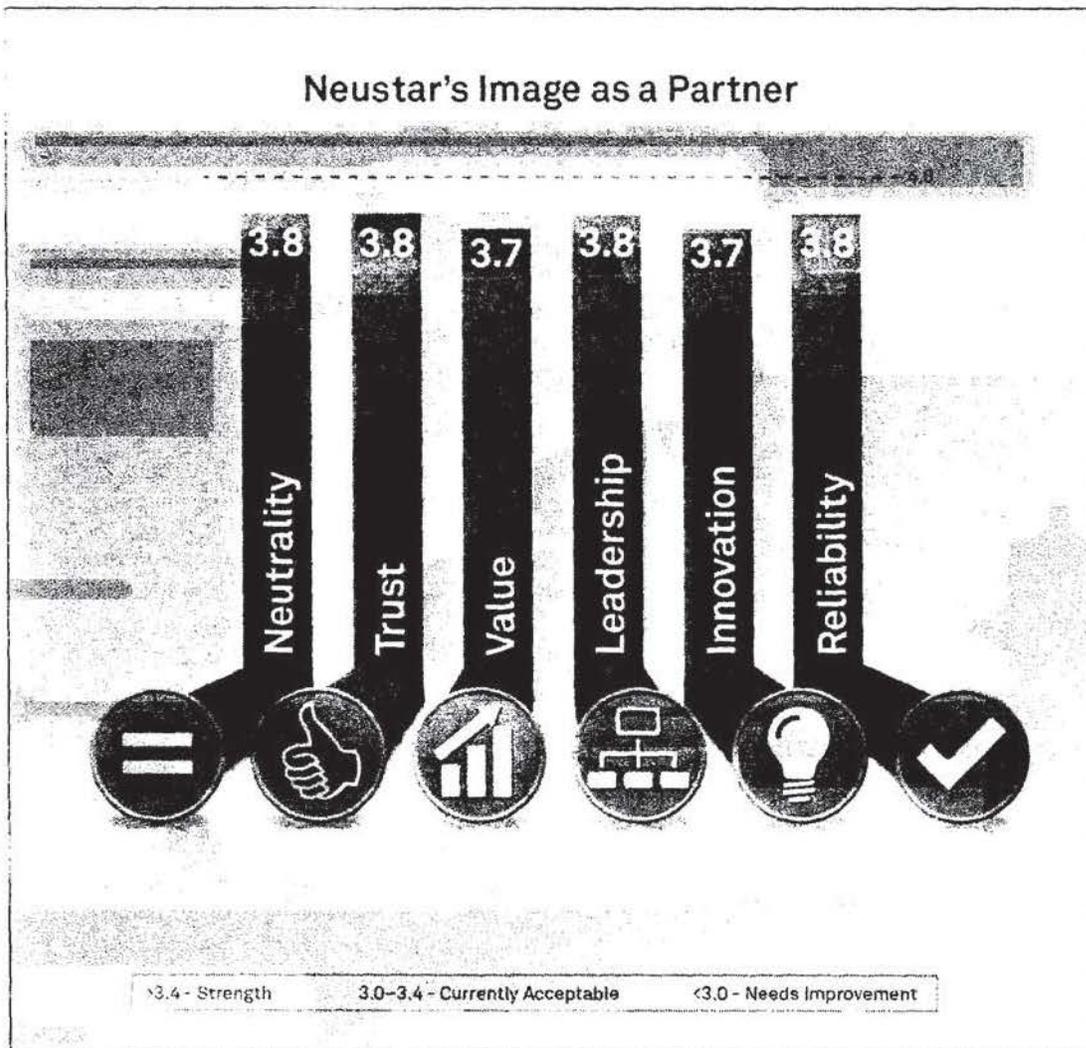


Exhibit 1.3-7: Results from Neustar’s 2012 NPAC User Survey, performed by a third-party, demonstrate our commitment to operational excellence.

## 1.4 Neustar's Security Program

---

### Why Neustar

- Security-Related Information
  - Neustar security program uses the "defense-in-depth" approach, leveraging multiple layers of security to ensure system and information resiliency
  - Neustar adheres to Industry best practices for securing information and systems
  - Continued training and education for security experts to remain ahead of emerging cyber threats, and ongoing Information Security training and awareness campaigns for all Neustar employees
  - Security operations are all based in the United States

### New for the Next Term

- Improved "threat intelligence" and response capability for NeuCIRT/SOC in 2013
- ISO27001 information security certification for NPAC
- Continued investment in the Information Security program to ensure Neustar stays ahead of emerging threats (people, processes, and technologies)

---

Neustar's approach to information security is a comprehensive, defense-in-depth program designed to mitigate all types of information security risks, while constantly evolving to stay ahead of the ever changing cyber threat landscape. Enabling secure customer access and protecting customer data are the primary goals of our information security program.

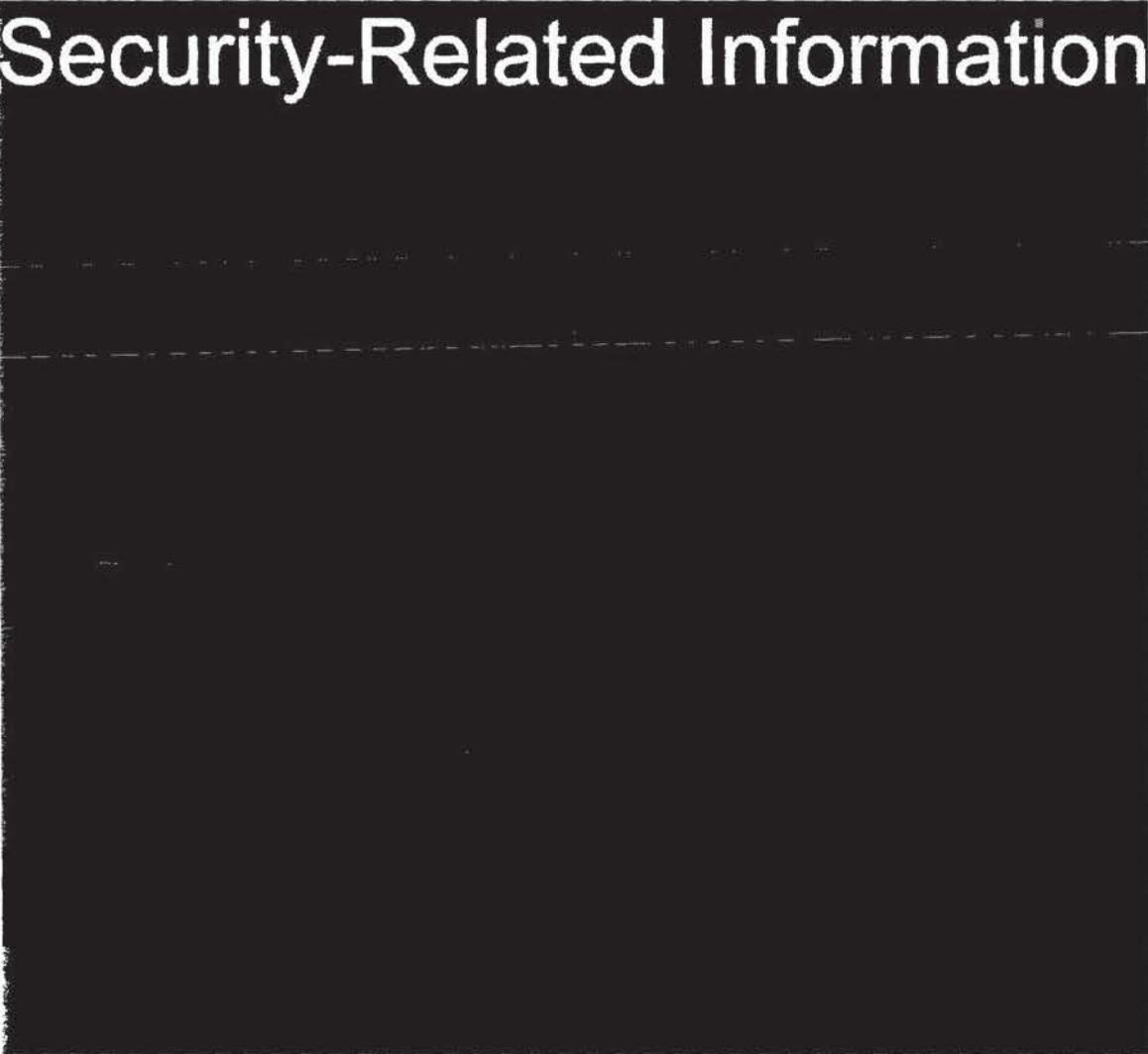
Over the past several years, the world has seen a huge increase in both the number and complexity of cyber attacks against governments and business enterprises. Regardless of the motivations behind these ever-changing threats, Neustar has taken the necessary steps to not only protect against these threats, but to stay ahead of them. Through a robust, defense-in-depth corporate information security strategy, which encompasses requisite preventive, detective, and corrective security measures, along with a proven Information Risk and Compliance program, Neustar is well prepared for these current and emerging cyber threats. These programs were designed to protect Neustar and our customer's information systems and data, while providing a secure means for customer access. Leveraging people, processes, and technologies, Neustar continuously assesses current capabilities against emerging threats and regularly updates security and privacy controls to ensure operational resiliency.



Neustar uses resources across the organization to quickly and effectively respond to information security threats. The following are highlights of some of our overarching principles and practices:

- **Defense-in-depth approach**—Neustar embraces a defense in in-depth or layered approach to security including strong physical, technical and administrative security controls. As shown in Exhibit 1.4-1, Neustar uses a diverse selection of security tools and vendors, which eliminates risk of any one vendor-specific security vulnerabilities.
- **Threat intelligence capability**—Neustar understands the ever-changing threat landscape and the increasing number of complex attacks being launched by hackers. In order to stay ahead of new attack methods, Neustar has implemented a “threat-intelligence” capability that provides us with improved zero-day (a previously unknown vulnerability in a computer application, meaning that the attack occurs on “day zero” of awareness of the vulnerability.) malware detection through advanced threat-feeds.
- Security-Related Information
  
- **Continued training and education**—Neustar’s information security team keeps up with the latest security best practices, by attending training, conferences, and networking with other security professional in various companies via industry working groups, organizations, and events. In addition, our security experts provide mandatory annual Information Security Awareness training for the entire work force.
- **Industry best practices**—Neustar’s information security and risk management program aligns with the ISO27001 standards and National Institute of Standards and Technology (NIST). Neustar is currently preparing for the ISO27001 certification for the NPAC. The NPAC infrastructure is currently ISO9001:2000 certified.
- Security-Related Information
  
- **Regular audits**—Neustar is subjected to regular audits such as: Sarbanes Oxley, SSAE16, ISO9001:2000, and self-imposed internal audits.

# Security-Related Information



## Security-Related Information

### 1.4.2 Information Security Framework

Neustar's Information Security Framework consists of sophisticated measures that both proactively defend against attacks as well as rapidly respond to them for minimizing the impact of any attack. Security-Related Information

Our detective and corrective measures are implemented and managed through the Neustar Cyber Incident Response Team/Security Operations Center (NeuCIRT/SOC).

Neustar's information security starts with comprehensive policies and standards utilizing industry best practices, including ISO and NIST. Policies and standards are reviewed semi-annually and updated as needed. Through adoption of recognized standards and the utilization of proven security solutions, Neustar has a cohesive and highly effective approach in protecting against data loss, targeted advanced persistent threats, and distributed denial of service attacks.

We have implemented enhanced security monitoring and threat prevention by developing a variety of techniques and systems to maintain awareness of emerging techniques and tools in the hacking community. Security-Related Information

Neustar recognizes the vital need to secure the systems and the integrity of the data in commercial solutions. Our extensive background in carrier-grade solutions has led us to install and operate computing and communications systems in accordance with solid business and security practices, including the consideration of physical, network, server, and application elements.

### 1.4.2.1 Information Security Framework—Preventive Controls

As the old saying goes, “an ounce of prevention is worth a pound of detection,” preventive measures are always better than a cure. Preventive-based security controls provide a higher level of efficiency whereas detective and corrective based security control is usually much more costly. While Neustar maintains solid detective/corrective controls, the foundation of the security program (shown in Exhibit 1.4-2) is built on time-proven preventive controls (administrative and technical).

Security-Related Information

• Security-Related Information

# Security-Related Information



## Endpoint Security

Neustar's security teams have deployed a comprehensive approach to security for the endpoint: employee desktops, laptops, and other devices. Employee desktops and laptops are one of the largest targets for hackers, viruses, and malware. To safeguard our endpoints, we have deployed proven technologies in a defense-in-depth approach, which directly increases the security posture of NPAC. Some of the key security capabilities that protect the NPAC environment include:

- Security-Related Information

- **Security awareness training for the workforce**—Neustar firmly believes that employees are the first line of defense against security incidents; therefore, we have successfully developed a “culture of security” environment. Through specialized security and awareness training and focused security forums, employees are made aware of security-related threats and potential attack vectors (i.e. vulnerable applications, phishing attacks, social engineering, etc), thus providing an additional line of defense against malicious security activities.

- Security-Related Information

- **Network access control**—Neustar utilizes network access control (NAC). NAC gives us full visibility to every system on the network and allows us to limit access for different classes of users with the use of policies.

- Security-Related Information

### Operating Systems Security

To protect our operating systems, we utilize the following preventive system controls:

- Security-Related Information
  
- **Patch management**—Neustar's formal patch management program was implemented to not only ensure timely security patching of systems, but also to provide improved system performance and compliance with regulatory requirements.

### Identity Management Security

Neustar has implemented a comprehensive set of technologies to form our Identity and Access Management Program. This program has allowed us to centrally control the lifecycle of all identities in the NPAC. Security-Related Information

- Security-Related Information
  
- **Web access**—Neustar offers Web Access Management and Policy controls to ensure only authorized users can access protected resources and generate SSO tokens for seamless session experience. Security-Related Information
  
- **SSO**—Neustar offers a secure SSO capability to its partners or customers. Internal identity federation provides a standards-based approach to bridging identity silos and application domains. We support all federation standards such as SAML, OAuth, WS-Federation, STS, OpenID. Security-Related Information
  
- **Centralized identity management**—Security-Related Information  
 This allows us to manage the life cycle of accounts more efficiency and gives us greater control over individual's access. Neustar practices the principle of least privilege for all accounts. Security-Related Information

Security-Related Information



Security-Related Information



## Security-Related Information



# Security-Related Information

- Proactive threat research on emerging threats
- Security-Related Information
  
- Focused reporting and briefings for advanced cyber threats and activity
- Security-Related Information

- Security-Related Information

## Security-Related Information



### 1.4.3 Information Risk and Compliance

Neustar recognizes that effective security management includes not only technical and tactical defense, but also a security approach that encompasses security risk management and compliance to further strengthen Neustar's infrastructure.

With increasing global threats to financial and information related industries, Neustar has enhanced its current security program to include an IT Risk and Compliance group (ITRC)—see Exhibit 1.4-4. This is a group of highly skilled professionals with decades of information risk and compliance experience in the telecommunication, new media, Internet, and government sectors. Security-Related Information

In addition, the Business Continuity Management (BCM) program strategy (see Proposal Section 1.2.4) and execution is managed with oversight from the ITRC.

Security-Related Information

# Security-Related Information

- **NPAC Technical Neutrality Audit**—Focus is on industry neutrality. Neustar provides a spotless record on neutrality and has passed all third-party audits of Neustar's neutrality. We are the only entity to have our neutrality confirmed in a Commission order.
- **NPAC Article 14 Audit**—Focus is on NPAC data center and operations in comparison with industry best practices. An independent, intensive third-party review of Neustar's NPAC data center and operations has found that these areas have consistently exceeded or far exceeded industry best practices in all tested areas year-over-year, including both Business Continuity Management and Security. See Exhibit 1.4-5 for our industry best performance record with regard to security for the NPAC.
- **ISO9001**—Focus is on NPAC's Quality Management System and documentation subject to a yearly external audit. Results from the annual ISO 9001 quality audits show consistent high performance and continual improvement.
- **Sarbanes-Oxley (SOX)**—Focus is on revenue, financially significant lines of business and systems. Neustar consistently has maintained a stable and compliant control environment, utilizing the COSO and COBIT frameworks. Since Neustar's public offering, Neustar has not had a materially significant deficiency found during any Section 404 testing for Sarbanes-Oxley.

### Security–Article 14 Audit Scores

Category	2009	2012	Trend
Security Overall Score	4.50	4.50	↔
Security Governance	4.30	4.37	▲
<i>Security Policy</i>	4.30	4.50	▲
<i>Security Awareness Training</i>	4.40	4.40	↔
<i>Security Compliance</i>	4.20	4.20	↔
Firewall	[REDACTED]		↔
Remote Access			↔
Network Security			↔
Host Systems & Database Security			↔
Data Center Security			↔

5 - Excellent performance, far exceeds industry best practices  
 4 - Above average performance, generally exceeds industry best practices  
 3 - Average performance, meets industry best practices  
 2 - Below average performance, fails to meet industry best practices  
 1 - Poor performance, falls far below industry best practices

**Exhibit 1.4-5:** Third-party audits validate our performance and provide valuable input on possible future enhancements.

- **Managing the Quality Management System (QMS)**—This is comprised of highly skilled information security risk and compliance specialists. The QMS ensures an objective, independent review of internal processes, controls, and practices across the enterprise. Our ISO 9001 certification validates the effectiveness of the QMS.
- **Leveraging third-party automated tools to ensure high-quality performance**—Neustar has implemented an industry-leading Security-Related Information The use of such automated tools provides for further  
business agility while providing risk, vulnerability, compliance, business continuity, and disaster recovery metadata management and tracking.

Oversight not only includes information security, but also business processes, documentation, physical and environment controls, and other areas of the company that may have a downstream effect on the information and operational environments. Through a layered approach, Neustar's technical, administrative, and physical controls are designed to ensure Neustar's assets are properly protected, operate effectively, and remain in compliance with legal and regulatory requirements.

### **Information Security Risk Management**

Neustar recognizes that security risk management is a critical component of its operations at the corporate and business unit levels. To properly manage corporate assets and to serve customers as expected, Neustar has incorporated regularly scheduled security risk assessments of its business units. The probability of each risk is assessed and an overall inherent risk rating is derived. The process considers both external and internal risk factors on each business unit, and management's capability to focus on the impact of those factors on operations. The findings from the information security risk assessments are distributed to our senior leadership and incorporated into the Neustar Enterprise Risk Management (ERM) reports, as required.

Neustar has implemented an integrated approach to information security risk management throughout the enterprise. Under the leadership of Security-Related Information the information security risk management teams are well positioned to provide the requisite oversight to ensure risk-benefit analyses, and security are applied throughout the risk management process. Neustar's assessment methodology is based on industry specifications such as ISO27001, ISO27005 (shown in Exhibit 1.4-6), and the newer ISO31000 standards, which allows for a comprehensive approach to be applied in the evaluation of mission security risks, including the identification of proper protections to safeguard information systems and customer data.

- **Security-related information**

# Security-Related Information

• Security Related Information

## 1.5 FUTURE NPAC/SMS INNOVATIONS

---

### Why Neustar

- Neustar’s proposal addresses the most complex challenges facing the industry in the next contract term, including:
  - PSTN Transition to IP Networks
  - Telephone Number Security and Authentication
  - Information and Analytics
- Expanded capabilities and services, all driving incremental value to Service Providers and consumers, including:
  - The creation of a comprehensive national IP interconnection registry
  - Standards-based M2M number administration and exhaust prevention
  - Cross-provider Equipment Registry to track and disable stolen devices
  - Transparent enablement of fixed-line telephone numbers for SMS interoperability
  - Certificate authority for TN-based communications over IP
- Neustar’s proposal offers NPAC/SMS Users access to ElementOne, Neustar’s market-leading data visualization and reporting platform, to provide complex analysis of NPAC/SMS data

---

Neustar possesses an unmatched foundation of technical and management expertise, and a 15-year record of partnership with the Industry in addressing Service Provider challenges. Neustar experts are often the Industry’s and the FCC’s first call with respect to the way consumers and Service Providers interact with telephone numbers; together we have collaborated on issues as diverse as expanding portability requirements, telephone number conservation, public safety, and third party telecom compliance. In recent years, we have accelerated our corporate investment and market leadership into high-availability data center operations and cyber-security, as well as NPAC/SMS feature functionality, all to provide a best-of-breed approach that consistently exceeds customer expectations. Over the next contract term, the investments Neustar continues to make will provide an irreplaceable foundation for the Industry’s requirements—designed to unlock material cost savings and revenue opportunities for Service Providers, and to facilitate maximum benefit to consumers.

Telephone number administration, addressing, and assignment in North America will undergo a significant reinvention over the next ten years, progressing in parallel with Service Providers’ unprecedented investment into all-IP network infrastructure. The resulting transition will be as transformative as that which introduced local number portability in 1997. As telecom services increasingly assume the benefits and burdens of IP technology, and the volume of connected devices skyrockets into the billions, Service Providers face a decade of disruption with regard to

business processes, interconnection protocols, and regulatory compliance. The NPAC/SMS will facilitate this transition by integrating capabilities to enable IP Interconnection, M2M, and authentication, as well as extensions to support number administration for the next decade.

This section of our proposal provides an overview of the market and regulatory drivers that drive Neustar's proposed NPAC/SMS roadmap, along with the projected value to the industry of our investments and innovations. The proposed enhancements each rely upon and assume the NPAC/SMS's unique architectural foundation and neutral governance, can be implemented with full backward compatibility, and will trigger no involuntary transition cost for the industry. We have focused our attention onto three related areas of opportunity:

- 1. Public Switched Telephone Network (PSTN) to IP Transition**—The Industry is investing billions of dollars in migrate to IP infrastructure to support consumers' ever-increasing demand for mobility, personalization, and convergence. At the same time, an unprecedented influx of devices connected to cellular networks is expected to rise over the next decade. These events require a rethinking of how telephone numbers are assigned, administered, and authenticated in next generation networks and back offices. In order to fully realize the value of the transition, to the industry will need to evaluate the PSTN's various geographic constructs will be required as Service Providers define optimal points of network interconnection to accommodate subscriber growth and mobility. More efficient and cost-effective utilization and forecasting procedures can replace many of today's procedures, saving Service Providers significant costs of administration. The NPAC/SMS is the most sophisticated and powerful of the Industry's assets to address this next reinvention of numbering, and will provide a bedrock foundation to support this critical Service Provider transition.
- 2. Telephone Number Security and Authentication**—Consumers, enterprises, and even machines rely upon telephone numbers to direct sensitive transactions even beyond communications—for example, mobile finance, health care, and home security. This evolution, while heralding significant value for Service Providers, also raises the specter of new challenges with respect to identity verification, fraud, and abuse. As IP technology becomes more prevalent, it will become easier and cheaper to spoof telephone numbers (and by extension, impersonate individuals and businesses) in communications traffic. The NPAC/SMS provides a common platform to define and execute standard features for telephone number security and authentication (for example, digital certificates signifying duly assigned ownership). This will ensure that as telephone numbers increasingly migrate onto the Internet, opportunities for misrepresentation and other mischief can be discouraged and mitigated.
- 3. Information and Analytics**—The NPAC/SMS is currently an invaluable source for information related to subscriber acquisition, network utilization, and number inventory management. Even so, extracting the kinds of meaningful information that can facilitate better business decisions can put a material burden on Service Providers' IT departments. Neustar's unique understanding of our customers' needs has already led us to develop market leading information services tools for the Industry, which we have made available at little to no cost. As part of the next contract term, we propose to expand that value by offering NPAC/SMS users access to Neustar's proprietary data visualization and reporting engine, ElementOne. ElementOne allows users to request and customize highly complex and user-friendly views into their NPAC/SMS data, including geographical and time-based trending reports.

All the requirements described in this section are considered subject to review and refinement by the LNPA Working Group and the NAPM, LLC. Notwithstanding the Industry's role to develop, certify, and approve detailed requirements, Neustar's proposal, by way of fixed annual SOW allocations from which the Industry can draw, includes implementation and deployment of any required NPAC/SMS changes at no incremental cost to Service Providers.

### 1.5.1 PSTN-to-IP Network Transition: Telephone Number 3.0

Telephone Number (TN) administration in the U.S. is on the brink of its second major evolution in twenty years. When it was first designed, the ten digit North American telephone number (NPA-NXX-XXXX) acted purely as a network address—geographically segregated, directly translatable to network routing instructions by virtue of its dialed digits. Numbers were allocated to Service Providers in blocks of 10,000 for a small geographic area—regardless of the need—because originating networks were programmed to interpret the first six digits of a number (NPA-NXX) to identify the location and owning Service Provider of every number in the country. A device's TN was directly linked to the Service Provider and switch location to which a call to that device would be delivered. We refer to this generation of telephone numbers as "TN 1.0."

Following the Telecommunications Act of 1996 and the introduction of number portability, this direct link between the number and the network was broken, moving the industry into the second phase of telephone numbers, or "TN 2.0." This was possible thanks to the implementation of Location Routing Number (LRN) technology. LRN technology changed the way networks operated in the U.S., impacting the way virtually all calls are completed. In the TN 2.0 network, a telephone number's dialed digits can be overridden by different routing instructions, assigned by the called party network as a result of a competitive port or a network modification. This was a fundamental change to call routing, necessitating upgrades to switches, inventory platforms, billing systems, and Service Provider interoperability; it fundamentally altered the way telephone numbers were administered and assigned in North America. Most significantly, LRN required the deployment of the NPAC/SMS, which subsequently became a critical element of the U.S. communications infrastructure, and provided the American consumer with a pronounced economic benefit in the form of number portability.

The Act of 1996 led to acceleration in demand for telephone numbers from the North American Numbering Plan (NANP). Because numbers were allocated to providers in large blocks, the threat of number exhaust became significant. To address that potential crisis, National Number Pooling was introduced in 2002, vastly improving the efficiency of telephone number assignment and extending the life of the NANP by decades. Today, thanks to the innovations in TN 2.0, the NANP is more resilient than ever, customers receive the benefit of choice and competition, and Service Providers have an asset in the NPAC/SMS that supports efficient and cost-effective network management.

Soon however, the industry's methods and practices around telephone number administration and assignment will require another evolution—one driven by another round of market and technological change in the communications industry. Increasing demand for mobility, personalization, and rich communications experiences has led Service Providers to begin the long process of moving away from the current TDM Public Switched Telephone Network (PSTN) infrastructure, and toward an all-IP infrastructure. For fixed-line carriers, the deployment of cable, copper, and fiber-based broadband technologies has paved the way for IP-based communications services to be delivered directly to consumers and businesses, replacing the older circuit-switched infrastructure. For wireless carriers, the industry's adoption of LTE and Voice-over-LTE (VoLTE) establishes IP as the central mechanism for core network management and transport, resulting in the convergence of multiple cellular protocols for the first time in the industry's history. Moreover, the widespread deployment of WiFi networks in public places and municipalities has extended IP-based communications to a variety of enabled devices and applications. Over time, as these islands of IP networks become pervasive, the need to interconnect them for seamless end-to-end communications becomes essential.

In light of the potential benefits to consumers from IP technology, the FCC is encouraging deployment of IP networks under the premise that certain core elements of the PSTN—universal access, Service Provider interoperability and public safety being paramount—be retained. In the FCC’s USF/ICC Reforms Order released in late 2011, the Commission encouraged Service Providers to interconnect using IP in addition to existing technologies. The FCC also has ordered the Industry to eliminate terminating access charges by the year 2018; this is the same billing treatment used today for pure Internet traffic.

In addition to rising demand on the network itself, the Industry is experiencing an explosion of connected devices; smart phones, e-readers, tablets, televisions, cameras, and a host of machine-to-machine (M2M). These devices support applications such as telematics, navigation, health care, energy conservation, and just about anything that developers can imagine operating over the telecommunications network. Over 500M connected devices are projected to be connected to the North American networks from homes, businesses, infrastructure, and vehicles by 2020—and a high proportion of these devices will require telephone numbers.

### Creating a Foundation for TN 3.0

All these developments imply changes to the way telephone numbers are administered, assigned to Service Providers, and used to authenticate devices and users on the network. TN 3.0 will involve three fundamental and related changes in the way the Industry interacts with telephone numbers.

First, the migration to IP networks opens opportunities for a more consolidated and efficient framework for interconnection. The PSTN’s geographical constraints on TN allocation and assignment (e.g. central offices and LRNs per LATA) will no longer be necessary, and will give way to the publication of IP endpoints for all TNs (designated either by Internet addresses such as URIs). This will lower Service Provider interconnection costs, enable more efficient routing between Service Providers, and open up new opportunities for efficient number utilization.

Second, TNs can be assigned to and returned by Service Providers as needed, based purely on the demand driven by consumers, enterprises, and connected devices on the network. As has been discussed by Service Providers in the past, Individual Telephone Number Pools can be established for IP-based Service Providers, to alleviate the need to allocate thousands blocks or Central Office codes for LRNs. This will extend the lifetime of the North American Numbering Plan indefinitely and provide maximum accommodation for growth.

---

### Why the NPAC/SMS

The NPAC/SMS’s unique characteristics make it essential as a foundation for TN 3.0

- Carries information to the 10-digit level, allowing TNs to be assigned to consumers and network routes without the constraint of fixed ranges
  - Built upon a real-time universal broadcast capability, with the power to authenticate and broadcast thousands of updates to the entire telecom network in seconds
  - Supports multiple interface options, including CMIP, XML, a web portal, and an expert-staffed help desk for manual tasks
  - Supports both PSTN and IP routing technologies, to support carrier needs for at least the next ten years
  - Guarantees neutral administration and prohibitions on commercial exploitation for all data shared by its Users
  - Operates under an fixed price business model with no incremental charges based on usage
-

Third, over time the complex processes for maintaining and synchronizing the nation's various numbering registries (NPAC/SMS, NANPA, SMS800, PA, and LERG) can be simplified and consolidated, eliminating the need for interfacing with multiple organizations and systems, and reducing Service Provider overhead.

The implementation and Industry adoption of TN 3.0 is a multi-year effort, requiring the collaboration of Service Providers, technology vendors, state regulators, and the FCC. In actuality, the process is already underway, signaled by discussions at the NANC, the INC, and the LNPA working group regarding the future of telephone numbers. Neustar, in cooperation with Service Providers and regulators, has begun to explore and address the requirements of registry consolidation and IP address exchange under the umbrella of TN 3.0. (See <http://www.neustar.biz/tn-3.0> for our presentation on TN 3.0, created by Neustar Fellow Tom McGarry, given in May 2012). Many of our customers have informed us that the highest priorities in the transition are to create maximum participation and adoption by Service Providers, at the lowest possible cost and risk of disruption. This is best accomplished by building upon the foundation of the Industry's existing numbering architecture and governance.

The NPAC/SMS already supports connection to all Service Providers in the U.S. over standard and secure interfaces, in an environment of high performance and neutrality. Extending the NPAC/SMS to accommodate the requirements for TN 3.0 will accelerate the benefits of Service Providers' IP transitions, while also ensuring full backward compatibility and maximum participation at no incremental expense. By comparison, the cost of building a new telephone number registry, defining new user terms and conditions, and integrating it with thousands of Service Provider IT and network systems could generate hundreds of millions of dollars in new capital and operational costs for the Industry.

Neustar's proposal for the next contract term includes, at no incremental cost, working with the various Industry groups to identify the appropriate pace and scope of the migration to TN 3.0, along with all development, testing, and deployment of Industry requirements. Given the broad implications, a subcommittee of the NANC and/or LNPA Working Group (which Neustar is prepared to lead) should be established to evaluate Service Provider perspectives and finalize requirements. The following sub-sections describe Neustar's current assessment of TN 3.0 benefits and requirements.

### **National IP Interconnection**

The first and most important requirement TN 3.0 must solve for is to develop an Industry-wide solution for translating TNs to Internet addresses. While both PSTN and IP networks are expected to coexist at least through 2020, IP will eventually replace TDM as the primary technology over which TN-addressed traffic is routed between networks. While LRNs can still be used to denote IP endpoints, most people familiar with this challenge have focused their attention on ENUM, a protocol created by the Internet Engineering Task Force (IETF) that converts a TN into an Internet domain name, and then uses DNS to obtain the Internet IP address for the point of interconnection (POI).

An ENUM-based solution is the best alternative for implementing Industry-wide IP interconnection in the near term (i.e., within 1-3 years). To create an Industry-wide ENUM solution for country code 1, Service Providers and technology vendors must not only rely on a common registry, but also collectively determine the appropriate provisioning, discovery, and authentication protocols. There have been attempts made over the last five years to establish such a function outside the NPAC/SMS—but none have succeeded, given the challenges of driving wide participation at manageable costs. The NPAC/SMS, however, already includes built-in, high-performing connectivity to Service Provider networks and back-office systems, and is likely to inspire wide adoption at the lowest possible cost. All NPAC/SMS functionality that is required to use the NPAC/SMS in this manner is already in place:

- Secure and reliable provisioning and distribution interfaces between all Service Providers
- Attributes to carry IP addressing information as well as for the PSTN
- Support for all North American telephone numbers (including non-ported and non-pooled, based on Pseudo-LRN technology).

Neustar has begun working with Service Providers and technology partners who wish to utilize the NPAC/SMS as the nation's common and trusted source for ENUM provisioning. In 2012, Neustar conducted the Industry's first trials to prove the viability of NPAC/SMS-based IP Interconnection. In 2013, in its role as a neutral third party and partner in collaboration, Neustar has begun establishing the requisite community forums to develop and foster the broadest possible collaboration and participation in IP interconnection. These forums, which include Service Providers from all segments of the market plus a number of strategic technology partners, will establish the appropriate data formats and protocols for the Industry to use the NPAC/SMS URIs.

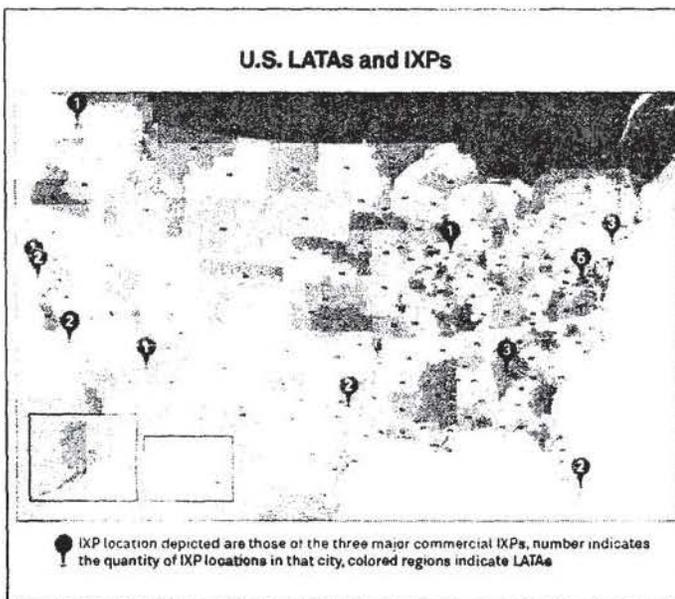
*\*\*For additional details regarding Neustar's proposed approach for IP endpoint provisioning, see attached white paper "Data Format Recommendations for Voice/SMS/MMS URI Fields in the NPAC."\*\**

### **Consolidation of Points of Interconnect (POIs) and Dynamic Route Provisioning**

In TN 2.0, LRNs are associated to Service Providers per switch, and per LATA—meaning that for each geographic area where a carrier provide service (approximately 200 nationwide), they must be assigned a 10K-block of TNs and must request an LRN. Maintaining these PSTN-based rules in TN 3.0 not only implies the use an ever rising quantity CO codes (leading to faster area code and NANP exhaust), but also forces Service Providers transitioning to IP to replicate the existing TDM infrastructure—that is, with an IP point-of-interconnect (POI) in every LATA across the country. This is unnecessary and inefficient.

Instead of insisting that there be one point of interconnect for each Service Provider per LATA, the Industry should use the transition to TN 3.0 as an opportunity to reduce the assignment of CO codes, and create greater flexibility for Service Providers to route calls based on the attributes such as location of the caller and agreements between the Service Providers – not simply based on the geography of the telephone number itself. IP-based Service Providers in particular do not require 200 POIs across the country; the assignment rules should recognize the potential efficiencies of allowing Service Providers to consolidate their POIs based on an optimal organization of the network. Exhibit 1.5-1 illustrates the difference between the number of LATAs (each requiring a PSTN point of interconnections) with the number of Internet Exchange Points, (IXPs) for three of the major commercial IXP providers.

This implies, over time, an elimination of the edits and business rules limiting telephone numbers and LRNs within geographically segmented boundaries. These edits have already been suspended on occasion (for example, following Hurricane Katrina), allowing telephone numbers to be assigned LRNs outside their LATAs. Over time, there should be no reason that an LRN cannot signify a point of connection on the IP network that terminates call traffic to multiple LATAs or even NPAC/SMS regions (presuming the NPAC/SMS remains national in scope, and is not divided among multiple vendors). Telephone numbers could then be assigned the appropriate LRN based not upon their dialed digits, but based on the locations, service characteristics, and behaviors of the subscribers to which they are assigned. When LRNs give way to URIs for direct IP addressing, the same principles hold—URIs have no fixed and published geography, they simply map to network endpoints as optimally defined by Service Providers.



**Exhibit 1.5-1: IP interconnections allows providers to limit the number of points of interconnection; compare almost 200 LATAs vs. 23 major Internet exchange points.**

In the last fifteen years, the NPAC/SMS has proven to be a highly reliable, always-on resource for the Industry, agnostic to underlying network technology for the telephone numbers under its stewardship. Recognizing this, a number of opportunities for cost savings and optimal routing are possible today that may not have seemed prudent during the initial NPAC/SMS deployment. One of these opportunities comes in the arena of dynamic, network-aware endpoint provisioning in the NPAC/SMS. For example, wireless Service Providers are currently in the midst of rolling out VoLTE application over their LTE networks, replacing the 3G infrastructure in phases. During this transition, which is expected to last several more years, mobile subscribers remain likely to move between 3G and VoLTE coverage areas with some frequency. Subscribers homed in VoLTE coverage areas are assigned LRNs that signal a device's eligibility for 4G coverage – and the LRN remains assigned even when those subscribers roam outside the VoLTE coverage area, and into a region still operating on 3G. When this occurs, terminating traffic will be sent first to the VoLTE network and then re-routed to the carrier's 3G network, using up capacity on gateway ports in the VoLTE network, and potentially degrading call quality. If, however, the wireless provider reacted to its subscriber's movement into the 3G area by publishing new routing instructions to the NPAC/SMS in real time, calling parties would then seamlessly begin sending traffic directly to the subscriber attached to the appropriate 3G network, bypassing the VoLTE network while the subscriber was out of the coverage range. Neustar has assessed the potential benefits of a dynamic route provisioning approach that reacts to subscriber movement, and has estimated industry savings of up to \$95M in reduced capital and operational network expense, depending upon the overall pace of migration to VoLTE.

*\*\*For additional details regarding Neustar's proposed approach for dynamic point-of-interconnect routing, see attached white papers "Enhancing NPAC's Role in Dynamic Addressing and Routing" and "Optimal VoIP Call Routing Using NPAC."\*\**

### **Accommodating the Demand from Machine-to-Machine**

One of the most recent sources of demand for numbering resources are connected devices, such as iPads, tablets, eBooks, etc. This is a precursor to a wider category of communications service known as machine to machine (M2M). M2M services cover a wide range of devices that have no direct human interaction, including meter readers, data collectors for utility services, sensors for health care monitoring devices, and more. Many of these devices operate over the cellular network, and therefore require the use of telephone numbers. These TNs are used for customer identification, billing, and auditing communications between M2M devices and application servers—but are typically not used for traditional voice and text interoperability.

Nearly 500 million M2M devices are expected to be connected to U.S. Service Provider networks over the next ten years—a potentially significant consumption of North American Numbering resources. This increase in demand could prove disruptive to the management of conventional telephone numbers, if not managed properly and with sensitivity to the consumer impacts of area code exhaust. Given the demand for M2M devices the Industry and the corresponding burden upon the NANP, the Industry is beginning to assess now the various mechanisms available to administer M2M numbering resources, and in so doing conserve geographic area codes.

Neustar has recommended, as part of the TN 3.0 evolution, that the Industry work to guide M2M-related demand to the 5YY series of non-geographic area codes, otherwise known as personal communications service (PCS) numbers. Demand for these resources has already begun to tick up, exhausting three PCS area codes in the past four years; to account for this, as a start 29 additional PCS area codes have been reserved in the NANP.

There are still limitations, however—today, non-geographic numbers are not addressable between Service Provider networks. This has implications for Service Provider billing and ordering platforms, and will require a solution to enable interoperability between networks (for example, consumers using SMS messaging to their home numbers to “wake up” energy saver or security devices). Neustar’s proposal involves the provisioning of 5YY numbers assigned to Service Providers in the NPAC/SMS, along with the ability to populate a new M2MURI field for the purpose of Service Provider interconnection.

Using the NPAC/SMS to allocate and administer non-geographic resources for M2M will permit the Industry to monitor usage and demand for these critical resources. In addition, since the vast majority of inter-Service Provider communication for M2M will traverse the IP network, the NPAC/SMS’s URI fields permit a secure, efficient, and auditable mechanism for exchanging endpoint information.

*\*\*For additional details regarding Neustar’s proposed approach for M2M, including how to leverage the NPAC/SMS to provide inter-carrier application services, see attached white paper “M2M Number Administration, Interoperability, and Service Enablement.”\*\**

### **Individual Telephone Number Pooling (ITN)**

The majority of telephone number demand over the next decade will be driven by mobile and IP-based service offerings, and by M2M. Currently, the FCC is considering mechanisms to allow pure VoIP Service Providers direct access to numbering resources. The best way to conserve consumer resources for the long term, and to pave the way for removing geographic constraints for telephone numbers completely, is to allow exceptions to the requirements of assigning carriers blocks of telephone numbers in large ranges limited to specific rate centers. The Industry, in collaboration with state regulators and the FCC, has the opportunity now to begin the process of

developing the means to allocate telephone numbers to carriers in direct proportion to their need. We refer to this concept as just-in-time assignment, or Individual Telephone Number Pooling (ITN). This concept could be offered initially for the use of interconnected VoIP SPs, and subsequently expanded to allow all carriers to participate. Over time, numbers could be harvested from existing stands of stranded numbers presently assigned to specific rate centers. The process would require national standards, which could be developed by the appropriate industry numbering committees with guidance from the FCC.

An ITN environment allows Service Providers the option of requesting numbers on an as needed basis, from a common pool stewarded by a neutral, non-Service Provider third party, such as the Pooling Administrator (PA) itself. These pools can be established in the NPAC/SMS with minimal effort within existing, unused ranges of TNs in designated area codes, including TNs from blocks with contamination levels too high to permit their assignment today.

Briefly, using largely existing functionality, the PA/NPAC/SMS telephone number assignment process can work as follows:

- Initial Start-up Activity:
  - PA will open ITN pools - telephone number ranges for specified rate areas in NPAC/SMS, under its own Service Provider ID (SPID)
  - NPAC/SMS will ensure each range of TNs opened for Service Provider assignments is available for immediate activation by addressing the "five-day, first-port notification" for the TNs' NPA-NXX
  - VoIP providers will apply for and be authorized by the relevant states to receive NANP numbers
  - NPAC/SMS will change the status of state-authorized VoIP providers from "read-only" to "read-write" for the applicable regions
  - VoIP provider will open an LRN in the NPAC/SMS, drawn from an NPA-NXX code assigned to its PSTN connectivity partner (a CLEC or other facilities-based provider).
- Number Assignment Process:
  - Upon new customer acquisition (not a competitive port of an existing number), the VoIP provider will submit a Create Pending SV request to NPAC/SMS, to obtain a TN for its customer from the common ITN pool. This Pending SV will have an LRN provided by its PSTN connectivity partner, and a VoIP URI for pure IP traffic.
  - The NPAC/SMS will send notification to PA about the ISP's Create Pending SV request.
  - PA will compare SPID making request with any other restrictions at the NPA or state authorization level.
  - PA will respond with "release" message to NPAC/SMS, with concurrence flag set either to "true" or "false".
  - If authorization fails, concurrence flag is set to "false" and VoIP provider is notified by NPAC/SMS that it cannot take the TN.

- Once due date and time on the pending SV are reached, VoIP provider can send an Activation request to NPAC/SMS. If Activation before the Due Date is desired, VoIP provider will first send a Modify Due Date request to NPAC/SMS. Once activated, the NPAC/SMS broadcasts the TN information to the rest of the Service Provider community and the telephone number is seen as now served by the VoIP provider.
- When customer terminates service, the VoIP provider will send a Delete TN message to NPAC/SMS. Deleting the record restores it to the PA's TN inventory in NPAC/SMS.

This entire process can be automated between the PA and the NPAC/SMS, resulting in an immediate assignment of the TN to the VoIP Provider.

Over time, and with the addition of the universe of carrier telephone numbers, ITN can significantly reduce the frequency of area code exhaust by maximizing the utilization of existing resources. That is, there is no requirement for VoIP providers to maintain inventories of spare numbers for assignment. In addition, utilization and forecasting can be accomplished far more efficiently, without each Service Provider needing to report on the consumption of pre-assigned ranges of TNs.

### **Beyond ENUM: Telephone Number Related Queries (TeRQ)**

ENUM was originally created as a consumer solution, not one for Service Providers to connect networks. When Service Providers moved to incorporate ENUM, they put requirements on it that were inconsistent with DNS. For example, they wanted it to be on a secure network, rather than the open Internet, and wanted to authenticate the originator of queries. These and other ENUM shortcomings are covered in a document titled Architectural Considerations on Application Features in the DNS, <http://www.ietf.org/mail-archive/web/i-d-announce/current/msg40967.html>, issued by the Internet Architecture Board (IAB) that is the oversight committee for the IETF.

In recognition of some of the long term shortcomings of ENUM, Neustar has been working on a long term solution for IP interconnect called Telephone Number Related Queries, or TeRQ for short. Jon Peterson, a Neustar Fellow, has been spearheading an effort at the IETF for creating a protocol independent framework and data model for queries related to telephone numbers and call routing that breaks through the limitations of ENUM, and can be a foundation for interconnection in the latter half of the decade. The latest draft is attached to this proposal, and can also be found at <http://tools.ietf.org/id/draft-peterson-terq-02.txt>. A presentation by Mr. Peterson given at IETF 85 in November 2012 can be found at <http://tools.ietf.org/agenda/85/slides/slides-85-dispatch-0.pdf>.

Neustar's proposal for NPAC/SMS administration includes evolution toward protocols like TeRQ, including aspects for both provisioning and querying. In the future, the NPAC/SMS can be expanded to include a field for a provider's TeRQ information server (similar to the way Caller Name functionality works today with the user of SS7 DPC parameters). Alternatively, the NPAC/SMS can be enhanced to serve queries directly over the TeRQ protocol for telephone number-related data such as geo-location, subscriber presence, and enhanced caller-id.

*\*\*For additional details regarding Neustar's proposed approach for TeRQ and its potential benefits to Service Providers, see attached white paper "Telephony-related Queries."\*\**

## 1.5.2 The Telephone Number as Identity in an Internet Marketplace

In addition to ensuring that telephone number administration keeps pace with and continues to provide essential value in an all-IP world, Service Providers are also uniquely positioned to expand their mindshare and wallet share by investing in the telephone number as a secure and reliable identifier for users on the Internet. Telephone numbers, unlike many other identifiers used over the Internet, are ubiquitous, globally unique, assigned as a public resource with neutrality in mind, and above all highly trusted. Service Providers' ability to efficiently leverage this key asset is critical, as they navigate the new landscape of non-traditional competitors and raised consumer expectations.

The first step is to ensure that telephone numbers retain their status as secure and reliable identifiers. With the proliferation of IP technology, it is becoming easier for entities to impersonate any TN as the calling TN. This is called spoofing, and is already a rising concern for Service Providers with regard to TNs. It is becoming quite common to spoof the originating telephone number for caller ID—in particular to deliver spam text messages and telemarketer calls. As VoIP and IP interconnection become more common, and as access charges are accordingly reduced, spoofing has the potential to increase in severity and volume. This problem is of great concern when one considers how TNs are used for two-factor authentication by web-based Service Provider, and given the reliance on TNs by the E911 public safety system.

This problem can be addressed via a standard, secure, and repeatable means of determining who owns a telephone number, and who retains responsibility for services originated from it. Interestingly, this problem of authentication is easier to solve in an all IP environment than it would be for just the current TDM network. The TDM network has the problem of "transitive trust", in which each entity in the chain trusts the entity previous to them. Often there's no direct trust relationship between the originator and terminator of a call.

On the Internet, however, digital certificates are commonly used between endpoints to ensure the veracity and trustworthiness of a transaction. They are used in DNS security to verify domain names, and in Resource Public Key Infrastructure (RPKI) to verify IP addresses. The same type of digital certificate, for Internet-based services, can be associated with a telephone number, which binds it to the assignee and allows third parties to assess the veracity of incoming transactions before completion. The TN can thus be authenticated at each link in the supply chain, including the end point.

Neustar's proposal includes an extension to its current interface to enable the association of digital certificates to NPAC/SMS resources, specifically to TNs. Since the NPAC/SMS is an authoritative registry, these certificates can be used to verify that the originator of any transaction is indeed responsible for the TN. Service Providers will be able to request that the NPAC/SMS issue digital certificates for any TN or range of TNs under their management, in such a way that will automatically keep pace with all porting and pooling transactions that impact Service Provider inventory. These certificates can be delegated to resellers and over-the-top providers, so that all elements of the telecommunications supply chain have the ability to securely and reliably authenticate their calls and messages from the TNs assigned to them.

Over time all TNs in the NANP can be associated with an NPAC/SMS certificate; this will reduce nefarious actors' ability to spoof a provider's TNs as a means of disguising their identities, thereby improving quality of service and reducing the impact on subscribers.

This concept can even be extended to serve as a consumer's identity in cyberspace. There are many companies—including but not limited to the same over-the-top Internet and social media providers currently acting as partners to Service Providers today—vying to be the consumer's primary provider of identity in cyberspace. These companies recognize the need for subscribers to aggregate personal information for mobile and IP-based transactions related to health care, finance, home security, and others, in such a way that is reliable and fully safe. The US government has even organized an effort called National Strategy for Trusted Identities in Cyberspace (<http://www.nist.gov/nstic/>) to evaluate this specific issue, and ensure that consumers have appropriate options as the technology environment evolves. The communications industry has an opportunity to proactively secure telephone numbers as a preferred subscriber identity for this very purpose—building upon their reputation as providers of high-performing, trustworthy, and reliable services.

*\*\*For additional details regarding Neustar's proposed approach for NPAC/SMS digital certificates, delegated authority, and identity management, see attached white paper "Telephone Numbers as Secure Universal Identifiers."\*\**

The concept of the NPAC/SMS providing an authoritative identity service in a changing market is further exemplified in two ongoing Industry discussions—SMS over fixed-line telephone numbers and stolen handset registries.

### **SMS Interoperability for Fixed-line Providers**

In recent years, non-wireless SPs and their partners have developed mechanisms to send and receive text messages, similar to the manner of wireless operators. This has allowed for a variety of new services and applications to be delivered, including SMS to the set-top-box, SMS to tablet clients, and integration with social media. However, it has also introduced a greater potential for fraudulent or abusive messaging to wireless customers.

Operators in the wireless and fixed-line communities, in cooperation with the CTIA, have in recent months been working to establish authoritative protocols for SMS interoperability for new entrants, particularly non-wireless providers with "over-the-top" resellers. The challenge has been to create a mechanism for transparent and authoritative whitelisting for telephone numbers that are eligible for SMS origination and delivery—with an aim toward maximizing the potential of interoperability between consumers, while minimizing the potential for spamming and spoofing in what is now a relatively clean ecosystem.

Neustar has recommended that non-wireless Service Providers use the SMSURI and/or MMSURI field in the NPAC/SMS to enable transparent, effective and efficient routing. Because the Industry already uses the NPAC/SMS for message routing for wireless numbers (by using a combination of SPID and service type), it is logical to include a designation within NPAC/SMS to identify non-wireless numbers that should be enabled for SMS.

With this protocol adopted, messaging aggregators and wireless providers will rely on a combination of SPID and SMSURI/MMSURI to derive a route for SMS/MMS. This approach will provide a consistent, transparent, and most importantly trusted mechanism to enable fixed-line carriers to offer messaging services in a manner that is transparent and secure, and that allows for prompt reaction on behalf of Industry in the event of identified spamming. The solution also helps to aligns messaging services portability with voice portability. The SMSURI/MMSURI fields are configurable to the provisioner of SMS service, allowing for flexibility with respect to the identity of the underlying user. Finally, all information relevant to service routing can be stored in an Industry-approved registry with equal, consistent access and appropriate oversight.

*\*\*For additional details regarding Neustar's proposal to use the NPAC/SMS SMSURI for whitelisting, see attached white paper "SMS Message Routing - Landline Numbers."\*\**

### **Equipment Identity/Stolen Handset Registries**

Given its ubiquitous connectivity across the Service Provider landscape, NPAC/SMS is the ideal location to store and distribute device identity and service information to serve the interests of the broader Industry. In particular, with the support of the FCC, the wireless community is moving towards a common platform to share information in a common Equipment Identity Register (EIR), to address fraud associated with stolen handsets. Individual carriers are currently moving forward with internal solutions, and the GSMA has begun offering a file transfer mechanism to support the exchange of information between carriers. However, no single platform exists today for U.S. carriers to not only publish this information quickly and efficiently, but also provision the information about stolen devices directly into their networks in the same manner as LNP data is provisioned today, using an LSMS-like infrastructure already in place feeding Service Provider networks. A nationwide platform to address stolen handsets can reduce fraudulent activity by reducing the value of stolen devices, and save Service Providers significant expense in opportunity cost and customer support.

*\*\*For additional details regarding Neustar's proposal to offer an Equipment Identity Register as part of the NPAC/SMS, see attached white paper "Equipment Identifier Registry (EIR) Solution."\*\**

### **1.5.3 NPAC/SMS and the Value of Information: The ElementOne Analytics Platform**

Today's number administrators and network engineers need access to the right information at the right moment, in order to maximize the effectiveness of their operation. Neustar's suite of analytics solutions gives Service Providers the power to make better decisions based on the data housed in the NPAC/SMS, for the essential purposes of network planning, telephone number resource allocation and assignment, and subscriber management.

The NPAC/SMS as administered by Neustar is already a source of invaluable reporting and analysis for NPAC/SMS users. The NPAC/SMS contains nearly half of the NANP's 1.5B telephone numbers allocated to Service Providers, and an even greater percentage of numbers in active service. It contains an authoritative picture of the movement of telephone numbers—and thus subscribers and devices—in and out of carrier inventories. More broadly, the NPAC/SMS also contains information that can illuminate the distribution and comparative density of telephone numbers across geographies and network facilities, along with the pace and trending of subscriber loss and acquisition. In total, over 12 billion data elements related to networks, subscribers, and telephone numbers are stored in the NPAC/SMS, all of which Service Providers have access to today for the purposes of routing, rating, billing, and network maintenance.

Over the last several years, Neustar has partnered with its customers to make NPAC/SMS data more accessible to users throughout a Service Provider's operations. To this end, we have developed the Port Power Search (Port PS) service, beginning with a free online service allowing authorized users to query individual or groups of telephone numbers and receive a consolidated ownership and routing disposition from all Industry numbering registries databases. Since its inception in 2006, Port PS has processed over 1.5 billion Service Provider queries, across over 14,000 Industry users - all at no charge. Recognizing the need for more, Neustar has since enhanced the Port PS platform with an online reporting tool known as Query Manager. The service offers a set of canned reports accessible to all users, and also offers the option of creating custom queries of a single virtual data model, that

includes all four Industry numbering registries (NANPA, PA, LERG, and NPAC/SMS). For the next contract term, and subject to review by the LNPA Working Group, functionality currently available in Port PS and Query Manager will be made available at no charge to all NPAC/SMS Users, as part of the NPAC/SMS User Agreement and accessible through the new NPAC/SMS Portal.

Beyond the incorporation of services with which the Industry is familiar through Port PS, Neustar also proposes to include, free of charge, access to our proprietary and market-leading analytics engine as a means to derive meaning and value from the NPAC/SMS's enormous datastore: the ElementOne Analytics Platform.<sup>1</sup>

### **The ElementOne Analytics Platform (EAP)**

Neustar's ElementOne (E1) is a robust, scalable, and secure cloud-based Geographic Information System (GIS) platform that provides rich data and cutting edge analytics to help clients make better business decisions. ElementOne leverages Security-Related Information, spatial and Java EE technologies to provide a feature rich, secure and highly scalable application to end users. Validating its best-of-breed attributes, in 2011 the EAP won the highly coveted Security-Related Information<sup>1</sup>, out of a field of leading domestic and international entries in the GIS Industry.

The key technical differentiators for EAP include:

- An Industry-leading cloud based geo-spatial query engine
- Sophisticated enterprise reporting, panels and dashboards
- Comprehensive and flexible area creation and manipulation functions (geography aggregations, non-overlapping component trade areas, configurable thresholds)
- Multiple topology views for accurate and granular geography relationships
- Improved base data precision with rate center, LATA, and ZIP+4 level data
- Cached tile maps for high performance, scalability and portability

---

<sup>1</sup> Although the implementation of a new NPAC feature relying on Neustar's proprietary ElementOne Analytics Platform technology as described in this Section 1.5 will be subject to the SOW Allowance process set forth in Section 3 of this Proposal, Neustar will, if selected as the LNPA, and as further accommodation to the Industry, exclude from the SOW Allowance calculation the cost of licensing the technology to users; provided, however, such underlying technology is not subject to any limitations or restrictions other than in conjunction with the provision of NPAC/SMS Services, the code to the underlying technology is not subject any escrow or additional licensing requirement, and the technology is not subject to any transition services obligation.

### **Information Services Available to all NPAC/SMS Users**

The E1 architecture provides a structured approach to assembling critical information, visualization and trending. In addition to offering automated, up-to-the-minute assessments of Service Provider inventories for the purposes of utilization forecasts and registry synchronizations, the E1 reporting and analytics package will offer, to all Users of the NPAC/SMS:

**Geographic Visualization**—E1 offers the use of clickable “heat maps”, which allows Service Provider users to navigate a clickable hierarchy of inventory or activity down to the Region, State, LATA, central office switch, and Rate Center level. The NPAC/SMS E1 instance will offer users a near real-time view into porting and pooling data, to quickly identify areas:

- Which have the highest inventory density relative to the surrounding areas and facilities
- Which have experienced higher levels of porting or pooling over configurable time periods
- Which are approaching inventory exhaust, necessitating requests for replenishment

**Histograms and trending reports**—While the heat maps described above excel at delivering a “snapshot view” based on geographical segmentation, the histogram function (also available as part of E1) allows for an even greater flexibility in organizing telephone number inventory according to configurable rules set by the Service Provider. In addition, E1’s access to historical NPAC/SMS data allows the user to create trending reports that show, over time, the pace of Service Provider activity with regard to the NPAC/SMS—competitive porting, pool block activation and donation, and network management. E1 can break this information down according to any attributes available to the analytics engine, including trading partner, customer type, service characteristics, or routing attributes (LRNs, URIs, etc.) As a mechanism to refine and streamline operations like provisioning and network management, the E1 analytics platform can be a valuable decision-making tool.

As part of the implementation of the NPAC/SMS Portal (described in Proposal Section 1.1), Neustar will request participation from the LNPA Working Group to discuss the specific configuration of the E1 platform for NPAC/SMS Users. Service Providers will only be able to run queries and perform analysis on their own NPAC/SMS data, and as a beginning, will only have access to data already stored in the NPAC/SMS. As the Industry evolves to TN 3.0, and Service Providers recognize a need to analyze the existing dataset against other, proprietary information in their own systems, the E1 platform can evolve to provide exponentially more value to Service Providers.

### Future Considerations

NPAC/SMS data is used subject to strict permitted use constraints. Pending review by the NAPM, LLC, Neustar is prepared to continue improving the information services and analytics that we can provide to Service Providers, both inside and outside the NPAC/SMS Administrator contract. NPAC/SMS data reflects the distribution and movement of telephone numbers nationwide—combined with other data sources, it can unlock material insights into networks, communities, and economies—with value not only to Service Providers, but also regulators and other public interest groups. For example:

- Neustar could combine aggregated and anonymized portability data with demographic and economic data, to identify correlations between telecom service and various types of population shifts
- Anonymized and Aggregated NPAC/SMS data can also provide insights into commercial data sources, to investigate correlations between telecom usage and other market trends in real estate, consumption, and job growth.

We look forward to continuing the discussion with the NAPM LLC on the value of NPAC/SMS-based information services in the next term.

### Conclusion

Over the past 15 years Neustar has developed and demonstrated expertise in managing a complex, highly available service to support Number Portability. This service is hosted on state of the art platforms, which have been refined over time based on years of unique operational experience. Neustar has continuously invested in the NPAC/SMS's reliability and availability, utilizing best of class commercial hardware, storage and software products. We have also repeatedly partnered with the Industry to invest in and refine our operational and business processes, all to accommodate consistently rising volumes and expanded services.

The telecommunications Industry will witness unprecedented change over the next decade, fueled by migration to IP networks, proliferation of devices, increased mobility, and further personalization of consumer services. These drivers underpin the importance and strategic relevance of NPAC/SMS innovation, building upon the unique characteristics that make the NPAC/SMS the Industry's most comprehensive and high-performing number management registry. Extending Neustar's partnership ensures that our current exceptional performance will be maintained, and further that the Industry will be able to focus on meeting the requirements of the future. Table 1.5-1 describes the various innovations and investments proposed by Neustar in the next term.

**Table 1.5-1. Proposed Innovations and Investments**

NPAC/SMS Roadmap Item	Value to Service Providers	Next Steps	Further Proposal Reference
National IP Interconnection	<ul style="list-style-type: none"> <li>Accelerated Industry adoption of standards and protocols for interconnection in a post-PSTN environment</li> <li>Avoids expense of building new numbering registry by leveraging existing NPAC/SMS architecture and governance</li> <li>All needed integration and application functionality present in existing NPAC/SMS</li> </ul>	<ul style="list-style-type: none"> <li>Further Service Provider trials with SOA/LSMS vendors and URI fields</li> <li>Definition of expectations and responsibilities for participating Service Providers</li> </ul>	Neustar white paper: Data Format Recommendations for Voice/SMS/MMS URI Fields in NPAC/SMS
Consolidated POIs and Network-Aware Provisioning	<ul style="list-style-type: none"> <li>Avoids need for central office / point-of-interconnect in each LATA, in favor of optimal network design unconstrained by PSTN geographic rules</li> <li>Efficient roll-out of VoLTE networks based on dynamic route provisioning as subscribers move between 4G/3G coverage areas</li> </ul>	<ul style="list-style-type: none"> <li>Policy discussion regarding LATA boundaries and TN / LRN assignment</li> <li>LNPA Working Group review (long term policy review)</li> </ul>	Neustar white papers: Enhancing the NPAC/SMS's role in dynamic addressing and routing  Optimal VoIP Call Routing Using NPAC
Individual TN Pooling	<ul style="list-style-type: none"> <li>Efficient use of numbering resources</li> <li>Reduced burden for utilization/forecast reporting for participating Service Providers</li> </ul>	<ul style="list-style-type: none"> <li>Continued policy discussion surrounding access to numbering resources</li> <li>Definition of PA and NPAC/SMS roles and responsibilities</li> </ul>	Section 1.5.1
Machine-2-Machine Administration	<ul style="list-style-type: none"> <li>Accommodation for significantly increased demand for TN resources. deferred area code exhaust (estimated expense for area code overlay)</li> <li>Increase value of M2M devices on Service Provider networks by maximizing interoperability options</li> </ul>	<ul style="list-style-type: none"> <li>Enable NPAC/SMS provisioning for non-geographic numbers (5YY)</li> <li>Add M2MURI attribute. M2M SV Type value to SVs and pooled blocks</li> </ul>	Neustar white paper: M2M Number Administration, Interoperability, and Service Enablement
TeRQ Protocol Enablement	<ul style="list-style-type: none"> <li>Offers a standard, authoritative, policy-rich query capability for Service</li> </ul>	<ul style="list-style-type: none"> <li>Continued Industry review</li> <li>Add TERQ URI attribute to SVs and pooled blocks</li> </ul>	Neustar white paper: Telephone Number Queries

NPAC/SMS Roadmap Item	Value to Service Providers	Next Steps	Further Proposal Reference
	<ul style="list-style-type: none"> <li>Provider information exchange</li> <li>Provides a template for post-ENUM interconnection and service enablement</li> </ul>		
TN Certificate Authority	<ul style="list-style-type: none"> <li>Increased security for TN-addressed messages over the internet (e.g. Caller ID, mobile finance)</li> <li>Opportunities for Service Providers to differentiate in the market for mobile Internet identity services</li> </ul>	<ul style="list-style-type: none"> <li>Definition of Certificate Authority procedures for use with NPAC/SMS interface</li> </ul>	Neustar white paper: Telephone Numbers as Secure Universal Identifiers
Fixed-line SMS Interoperability	<ul style="list-style-type: none"> <li>Expansion of fixed-line / over-the-top SMS providers (increased network effect and volume)</li> <li>Universal distribution of whitelisted telephone numbers to SMS ecosystem through LSMS broadcast</li> <li>Reduced spoof and spam thanks to authoritative and transparent NPAC/SMS population</li> </ul>	<ul style="list-style-type: none"> <li>Industry definition of standard syntax and guidelines for population and delisting</li> </ul>	Neustar white paper: SMS Enabling Landline Numbers
Equipment Identity/Stolen Handset Registry	<ul style="list-style-type: none"> <li>Reduced fraud due to stolen devices (13M estimated lost/stolen smartphones in 2013)</li> <li>Accelerated compliance with FCC requirements</li> <li>Leverages existing NPAC/SMS infrastructure and interfaces</li> </ul>	<ul style="list-style-type: none"> <li>LNPA WG review of NPAC/SMS enhancements</li> <li>Collaboration with GSMA to consolidate Service Provider option</li> </ul>	Neustar/Tekelec joint white paper: Equipment Identity Register Solution
ElementOne Analytics Platform	<ul style="list-style-type: none"> <li>Advanced analytics built on NPAC/SMS data,</li> <li>Improved decision making in support of business decisions related to subscriber acquisition, network management, inventory utilization</li> </ul>	<ul style="list-style-type: none"> <li>LNPA WG approval of Neustar recommended initial design</li> <li>Define license arrangement of proprietary platform software with NAPM, LLC</li> <li>Ensure compliance with permitted use restrictions for all NPAC/SMS data</li> </ul>	Section 1.5.3

## 1.6 Transition and Implementation

---

### Why Neustar

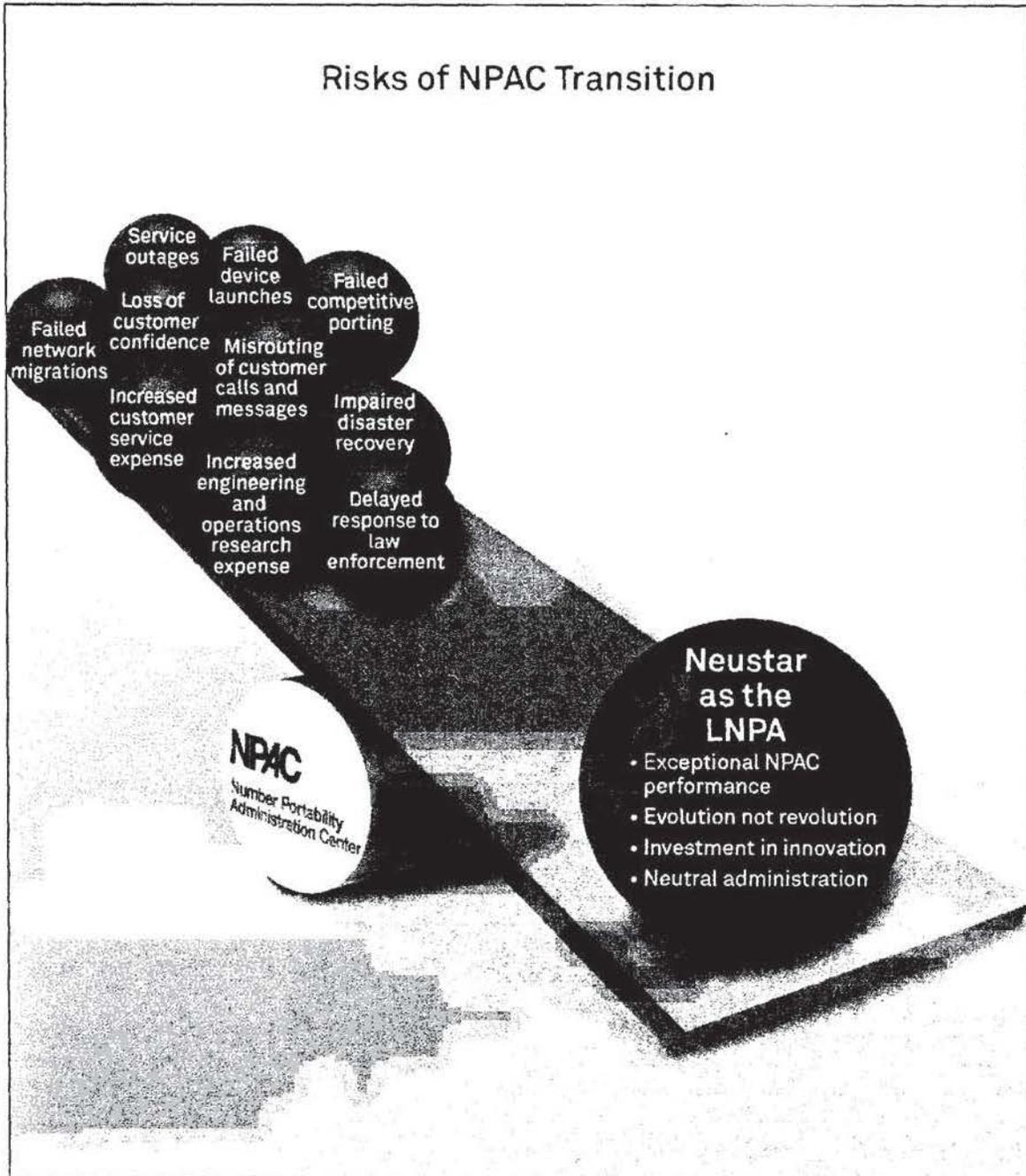
Any transition to one or more new LNP Administrators places great financial and operational risks for Service Providers and consumers. Retaining Neustar as the U.S. LNPA eliminates:

- ALL the risks and expense of an unprecedented industry transition, estimated to cost at least \$719 million for Service Providers
- Material opportunity costs for Service Providers and regulators, as resources are pulled from other strategic initiatives to focus on migrating the full set of LNPA services to a new, untested vendor
- Lengthy “shake-out” period of degraded service and periodic system unavailability - affecting consumers and driving up customer care expense
- Risk of failed calls and texts from even a small error in migrating the NPAC/SMS’s 12 billion data elements
- Potential for reduced readiness in times of disaster and emergency, when first responders and regulators rely on the LNPA to restore service
- Declining consumer porting experience, blocked access to numbering resources, and delayed or impeded network management activity – all of which are effected by NPAC/SMS performance
- Compounded Service Provider expense and uneven consumer experience caused by multiple LNPAs
- Loss of consumer and SP confidence in the LNPA’s understanding of and commitment to neutrality
- Reduced attention on strategic priorities (i.e. IP Interconnection) as alternate vendors focus on replicating Neustar’s performance rather than the needs of the future

---

The Industry understands better than anyone else that there is a lot at stake when contemplating a transition to another vendor for LNP administration. As highlighted below and in Exhibit 1.6-1, delays, issues, and failures in transition will have numerous negative consequences for the Industry with potentially significant impact:

- Misrouted telephone calls and misrouted traffic for services such as SMS/MMS messages, causing increased Service Provider customer service calls and associated costs; and if long-term, customer retention problems
- Failed or slowed competitive consumer porting with reduced or slowed revenue to Service Providers and increased Service Provider customer care and resolution costs



**Exhibit 1.6-1:** By selecting Neustar to serve the next term, the Industry eliminates all risks to the continuing success of Number Portability in the United States.

- Failed or slowed customer retention programs and new service/mobile device launches, again, with reduced or slowed revenue to Service Providers and further increased Service Provider customer care costs
- Failed or slowed access to telephone numbers for Service Providers
- Delayed law enforcement and public safety activity, putting citizens and property at risk
- Impaired disaster recovery efforts that use porting, pooling, or network migration as a remedy
- Failed or slowed Service Provider network migrations, potentially leading to customer service outages
- Improper calls made by automated dialers to wireless telephone numbers, causing complaints to the FCC and State PUCs

To provide another perspective for evaluators, Neustar sponsored the development of the following six studies published recently about U.S. LNP and U.S. LNP Administration:

1. *"Scale and Transactional Economies in NPAC Services,"* by Scott Masten, PhD—Professor of Business Economics and Public Policy, University of Michigan, which describes the advantages and cost savings provided to the Industry by having a single LNPA vendor nationwide.
2. *"Telephone Numbers Are Portable: Is the NPAC?,"* by the Yankee Group, which describes how LNP in the U.S. is a model for the entire world.
3. *"India's Experience with Mobile Number Portability,"* by W. Bruce Allen, PhD—Professor of Business and Public Policy, Wharton School at the University of Pennsylvania; Visiting Professor, Indian School of Business, which describes how the number portability ecosystem and infrastructure in the U.S. is vastly different and, in many ways superior to the number portability ecosystem and infrastructure in India.
4. *"Number Portability Through the Global Lens,"* by the Yankee Group, which concludes that there are vast differences between LNP ecosystems and implementations worldwide and there is no LNP ecosystem or implementation in the world that directly compares to the U.S.
5. *"The Consumer Benefits of an Efficient Mobile Number Portability System,"* by Hal J. Singer, PhD, Managing Director and Principal, Navigant Economics, which found that Americans have the fastest wireless number portability system in the world, resulting in billions of dollars in annual savings for wireless consumers. The report also found that any disruption to the number portability system's efficiency could potentially have a significant impact on wireless consumers.
6. *"Carrier and Consumer Impacts Due to a Change in Local Number Portability Administration,"* by Hal J. Singer, PhD, Managing Director and Principal, Navigant Economics, in the Attachments Section of our proposal, which discusses the risks and potential costs associated with a transition to a new LNPA vendor.

While Neustar, as the incumbent, is not required to provide a transition plan, we have included the following subsections to help the Industry evaluate a transition and a Respondent's transition and implementation plan—specifically an overview of what needs to be transitioned and evaluating plans including transition strategies.

### What Needs to be Transitioned

The transition to another vendor(s) is not a trivial task; it is not only all of the work and risk involved in implementing a technical infrastructure and transitioning the NPAC/SMS software and data and migrating both to their environment but also the transition or implementation and the continued operation of all of the services previously described in Proposal Section 1.1, LNP Administration Services. In addition, the following highlight some of the additional functions the LNP Administrator must manage and/or perform:

- Industry-wide customer satisfaction surveys
- Data and physical security functions
- Gateway Evaluation Process (GEP) and audits
- Business continuity planning and execution
- LNP Neutrality Audit, conducted by a third party
- Operations benchmarking and audit (Article 14 audit), conducted by a third party
- New User Evaluation (NUE) process, performed by a third party
- LNPA reporting to Industry and FCC
- Corporate functions like human resources, contract management, and training

Further, there are certain elements that are the foundation of Neustar's success such as practical expertise, NPAC/SMS customized processes, Neustar-developed tools, etc. that will not transfer; this increases the risk to the stability of the system and quality of service delivery. The following are two examples of what can go wrong and the potential impacts.

1. **Impacts to data integrity**—There is a large amount of data to be transitioned. For example, the NPAC/SMS database—across all 7 regions—contains approximately 600 million Subscription Version (SV) records, each with about 20 fields, meaning that there are 12 billion data elements that need to be converted and/or moved from the current seven regional NPAC/SMS to the new LNPA NPAC/SMS. Even a small error rate during the conversion or movement can lead to millions of potentially service-impacting, data integrity errors. These data errors likely will propagate over time to all downstream Service Provider LSMSs. Those errors will have to be dealt with in an ongoing fashion. Those are just the SV record data fields in the NPAC/SMS. There is other data in the NPAC/SMS and there is data associated with other systems such as the Billing and Collection system that must be converted and/or moved to any new U.S. LNPA during the transition period.
2. **Impacts to LNPA's Mass Update and Mass Porting (MUMP) operations**—Neustar has an experienced team that processes incoming MUMP requests. This team catches and filters potential errors affecting millions of transactions each year. Similar to the initial Subscription Version data conversion or migration, a small error rate of fractions of a percentage can lead to millions of data errors, which then impact telephony and information services and routing. These errors will have to be resolved on an ongoing basis. If a potential LNPA vendor does not possess a thorough understanding of the various U.S. LNPA service elements, like the MUMP service, they will become quickly overwhelmed, data errors will occur, and Service Providers and consumers will be negatively impacted.

## Evaluating Transition Plans

There are risks inherent in any transition of services and data from one entity to another. When that transition is between two different and unrelated entities, those risks, and their likelihood of occurring, are magnified based on differences in approach, expertise, culture, and agenda notwithstanding any contractual protections. Specific to this procurement, and to further complicate matters, the transition will have to begin and end in less than 15 months—an extremely short period of time. It is important to note that when procurement for LNPA services was first contemplated, there was an allowance of approximately 30 months of transition planning and execution time. A 15-month timeline is very tight and assumes no further delays to the procurement process. Further, this tight timeline is for not only a potential new vendor but also for the industry who must organize themselves to manage the transition. Therefore, in order for the industry to make the most informed decision and assuage any concerns regarding risk, it is critical a Respondent provide a:

- **Detailed, logical, well thought-out transition strategy** that outlines clearly how the Respondent's strategy meets deployment objectives with the least amount of risk and costs to Service Providers and ongoing LNPA operations
- **Comprehensive Transition and Implementation Plan** that details how the Respondent will execute on that strategy within the required timeline, with the least amount of risk and highest levels of quality

## Detailed, Logical, Well Thought-out Transition Strategy

Before Respondents identify the details of their Transition and Implementation Plan, they must make a few threshold strategic decisions. For example, they must decide:

- **NPAC/SMS Application Strategy**—Will a Respondent develop and deploy their own NPAC/SMS software or will it deploy the Neustar-developed NPAC/SMS software. If a Respondent proposes to use Neustar's NPAC/SMS software, then it must quickly become an expert in all aspects of Neustar's software, which software the Respondent did not develop. This is very risky. From time to time, Neustar does hire new software engineers to maintain the NPAC/SMS software and develop upgrades, updates, and enhancements to the application. However, depending on the experience of the software developer, it generally takes them between 9 to 12 months to be sufficiently trained to begin working on lower risk areas of the NPAC/SMS application. Because there are delicate inter-relationships between the hardware, network components, operating system, <sup>service provider</sup> , third-party system software, and the NPAC/SMS application software, there are areas of the NPAC/SMS application software where we allow only experienced software engineers who have been working on Neustar's NPAC/SMS for several years to maintain or work on.
- **Overall approach for initial service cut-over**—Depending on this decision, Service Providers and the industry are faced with either: 1) having the prospect of two LNPA vendors operational at the same time in the same region during the transition period or 2) having to cut-over all seven regions awarded to another vendor in a single NPAC maintenance window with no real ability to roll-back.

Unless the Industry does a high-risk flash-cut in one NPAC maintenance window of all seven NPAC regions, a transition from one LNPA vendor to another vendor will have to occur over an extended period of time, bringing with it nearly all the attendant problems and costs with having two LNPA vendors throughout the transition period.

The Industry is well aware of the direct and indirect costs to Service Providers caused by having two LNPA vendors. These well-documented, well-understood risks and costs are at a minimum those associated with the following. Neustar submits that Respondents can solve for some of the direct Service Provider transition costs; they cannot cover indirect costs and their plan should detail clearly how they would mitigate the risks:

- Service Provider efforts to connect their SOAs and LSMSs to multiple live LNPA NPAC/SMS platforms and test beds and maintain those multiple connections
- New software release deployment complications
- New carrier feature deployment complications
- Failover testing complications
- Internal Service Provider operational complexities in receiving services from two different LNPA vendors:
  - Help desk services
  - Reporting services
  - New User services
  - Tunable parameter maintenance
  - SPID migration limitations and process coordination
  - Resolution of differences among LNPA software implementations, some of which could be service-affecting
  - Data and information from multiple LNPAs into one LNPA WG Website coordination
  - Neutral change management administration
  - Development of Service Provider internal processes to accommodate differences in multiple LNPA M&Ps
  - Access, coordination, and management of Enhanced Law Enforcement Platform and Intermodal TN ID Service by multiple LNPAs
  - Negotiation, execution, and reconciliation of differences in Master Agreements with multiple LNPAs
  - Duplication of effort in changes under statements of work for modifying the NPAC platforms

If a Respondent's transition strategy is to propose a "staged transition" that takes place over time during the 15-month timeframe, that vendor needs to answer many of the questions posed by the Industry in RFP Section 14.1. These answers should be included in their submitted Transition and Implementation Plan as a part of their proposal. If the Respondent does not answer those questions then the Respondent does not understand the requirements and complexities of transitioning and operating a complex service like U.S. LNP Administration and is not up to the task of being the new LNPA vendor.

### **Comprehensive Transition and Implementation Plan**

The old adage "Failing to plan; planning to fail" applies to NPAC services as a whole and certainly applies to any transition of those important services and systems. This adage means more than the "mere existence" of a plan. This adage really means the "existence of a thorough, sound, and achievable" plan. If a Respondent cannot articulate a detailed and comprehensive, yet straightforward, Transition and Implementation plan, then it will have no chance of effectuating an error-free transition. A flawed transition will subject the Industry and public to all the negative consequence outlined above, some of which can cause irreparable damage and result in costs in the hundreds of millions of dollars. The Industry clearly understands this and has asked other Respondents to address the following in their submitted Transition and Implementation Plans:

- Anticipated overall transition period
- Implementation approach (e.g., tasks and milestones)
- Transition time intervals for individual functions and services
- Staff management approach (e.g., staff categories and hours per task)
- Risk management approach
- Change control approach
- Quality assurance approach
- A list of transition activities from the incumbent to the newly selected LNPA

These are minimum requirements.

In order to assist the Industry in evaluating submitted Transition and Implementation Plans, Neustar submits that any detailed, competently developed Transition and Implementation Plan should include:

- A transition strategy that mitigates as much risk to the Industry and their ability to effect porting
- An overall, logical high-level transition timeline which is realistic and achievable
- Reasonable assumptions/constraints regarding roles and responsibilities of the Industry, FCC, and incumbent
- A critical path analysis
- Sub-plans for the following that detail approach, tasks, resources, dependencies, durations, etc for each:
  - LNPA vendor neutrality
  - Database and facilities management
  - Service Provider connectivity

- Business continuity planning and execution
- Hiring/staffing/training that includes:
  - Job descriptions
  - Number of personnel already available and those that need to be hired before and during the transition
  - Associated job-related training on LNP Administration, NPAC/SMS development and operations, etc.
- Risk management/mitigation
- Communications plan to address inquiries: from the FCC, State PUCs, Service Providers, and other interested parties
- Roll-back to include detailed steps to roll-back operations if initial regional cut-over(s) fail and steps to test the initial cut-over roll-back procedures?
- Work breakdown structure that details tasks, durations, dependencies, resources to:
  - Transition all systems used for NPAC/SMS services—NPAC/SMS, Test Bed, Billing and Collection, Automated IVR, npac.com, LEAP, Intermodal Ported TN Identification, CRM (Help Desk and Trouble Ticketing)
  - Safeguard and guarantee data integrity of all current and historical data used by all NPAC/SMS service components, including identifying and addressing potential data package
  - Procure all necessary hardware and networking equipment
  - Install and provision all of the necessary hardware and networking equipment?
  - Perform testing (e.g., connectivity, interoperability, Fail-over testing, acceptance testing)
  - Implement all LNPA operational functions identified in Proposal Section 1.1 LNP Administration Services and any additional services the Respondent is proposing to add
  - Implement the Gateway Evaluation Process and its Audits
  - Implement the NPAC/SMS Data Center Operations Audits and Benchmarks
  - Implement the New User Evaluation process
  - Implement LNPA reports to Industry and FCC
  - Implement the Mass Update and Mass Porting (MUMP) service
  - Transition and modify all NPAC User Methods and Procedures

An incomplete or abbreviated transition plan indicates a lack of understanding of the LNPA eco-system and the impacts of disruption. Prospective vendors should not rely on the industry to solve the hard problems associated with migrating the NPAC/SMS. Given the significance of the LNPA service to consumers and Service Providers, the industry should set a high bar for confidence on the transition plan when judging whether a vendor's submission is technically acceptable.

### **Conclusion**

As depicted previously in Exhibit 1.6-1, the industry is faced with making a very important choice: retain Neustar as the LNPA vendor for the next contract term and continue receiving outstanding service with seamless upgrades and innovation without any transition risk, or select a new LNPA vendor, which by necessity, subjects Service Providers and consumers to substantially high risk in transition with numerous negative and expensive consequences. By selecting Neustar to continue to serve, the industry avoids **ALL**:

- Risk to the Industry, Service Providers, and consumers
- Service Provider costs associated with managing a transition
- Service Provider costs associated with operating in a multi-vendor environment
- Service Provider costs associated if the new vendor fails (amount dependent on type of failure)

## 2.0 MANAGEMENT FACTORS




---

### Why Neustar

- Continued investment in the Industry's top resources in numbering, portability, and network evolution
- Corporate heritage administering trusted, neutral third party services for diverse constituents
- Fully U.S. based and operated; not subject to foreign control
- Financially sound, publicly traded company with stable and diverse revenue streams and ample free cash flow
- Demonstrated commitment to absolute neutrality, based on a proven Code of Conduct trusted by the Industry and the FCC
- Experience administering the U.S.'s singular LNP requirements
- Highest possible rating for U.S. LNPA Customer Service since 2009, evaluated by external auditors and reporting a near-perfect 3.84 out of 4.0 overall satisfaction rating in 2012

---

U.S. LNP administration is a unique service, requiring a unique set of skills and experience to deliver it. The service provided by Neustar has no equivalent worldwide for its supported functionality; its diverse regulatory, Service Provider, and technology partner constituents; its performance under heavy and rising transaction volumes; and its myriad compliance and neutrality requirements. The NPAC represents critical infrastructure for the U.S. communications industry (Industry), and impacts the communications experience of millions of consumers a year.

- 500 million billable transactions on behalf of individuals and businesses in the U.S. in 2012 alone.
- The NPAC provides an invaluable layer of network resiliency in times of natural or man-made disaster, restoring service continuity using LRN technology.
- The NPAC is "always on", prepared to accommodate spikes in throughput to support Service Provider s' product launches and customer acquisitions with zero risk of disruption or degradation.
- NPAC personnel perform essential roles in all manner of Industry network management tasks, including customer cutovers, technology upgrades, mergers/acquisitions, and inventory assignments.

- Hundreds of competitive U.S. Service Providers rely on the NPAC as the primary source of their telephone number inventory; tens of millions of telephone numbers are activated and broadcast via the NPAC to support the national pooling process each year.
- Accurate NPAC/SMS broadcasts are essential to over billions telephone calls and text messages each and every day.

Degradation of any aspect of NPAC performance can result in disruptions to telecom competition, misrouted calls and text, inconsistent access to numbering inventory, and slow recovery from network outages or disaster. Service providers rely upon an available, high-performing NPAC to safeguard revenue opportunities, take advantage of network technology changes, and ensure regulatory compliance. Proposal Section 1.0, Technical Factors describes our service and technical proposal for the next term. This Proposal Section and subsections serve to describe the particular qualifications Neustar brings to the LNPA service, our corporate stability and commitment, our proven neutrality, and record of customer expertise we will to bring to bear to continue exceeding the Industry's expectations as it faces the challenges and opportunities of the next decade.

### Vendor Experience and Performance

Neustar is the only company worldwide with any experience providing LNPA services in the U.S. and is the Industry's unrivaled expert in numbering administration. We offer a broad suite of commercial numbering, order management, and IP addressing and routing services to all segments of the communications market. We are an essential partner to the FCC and state regulators for all topics related to the management and assignment of numbering resources. Neustar also possesses a corporate character and mission that is intimately tied to the principles of data privacy and security, as witnessed by our management team and product portfolio. Neustar's unrivaled neutral third-party administration credentials and our track record of successfully delivering scalable, reliable, and secure services are detailed in Proposal Section 2.1, Neustar's Corporate Experience.

### Financial Stability

The U.S. LNPA service processes millions of real-time transactions each day that are critical to healthy market competition and accurate call completion. As such, financial stability and corporate focus of the LNPA is paramount to the Industry's confidence and comfort. Neustar is large enough to offer stability and reliability, and small enough such that the LNPA service remains the primary focus of our company. We are a publically traded company that is fully U.S. owned and operated, as well as an independent company whose financial basis is not tied to a disconnected parent with a separate set of objectives. We possess a diversified revenue stream, and access to ample credit under excellent terms—illustrating the marketplace's confidence in Neustar's management and stability. Finally, we offer full transparency into our top level financials, through the quarterly attestations by our CFO, Paul Lalljie. As a testimony to our financial stability, we continuously provided outstanding U.S. LNPA service without disruption during both the Tech Bubble of 2000 and the Great Recession of 2008. For the next term, Neustar will not rely on 3<sup>rd</sup> party subcontractors for any material component of the LNPA service, offering the NAPM LLC and the FCC maximum visibility and confidence in our operation. As described in Proposal Section 2.2, Neustar's Financial and Operational Stability, we possess optimal financial stability with growing revenues, cash balances, and earnings per share to continue to provide superior U.S. LNPA service for the next contract term.

## Neutrality

Neustar was the U.S. Industry's first truly neutral, third party and, as such, not only do we understand it better than any other prospective bidder for the LNPA contract, we have fully embraced it as part of our culture and corporate character. As detailed in Proposal Section 2.3, Neustar's Neutrality, we have successfully passed 10 annual NPAC Neutrality Audits and 50 quarterly NANPA/PA (through 2Q'12) Neutrality Audits conducted by independent third-parties; we have submitted 60 Neutrality Reports certifying the results of these audits; we certify the neutrality of each of our over 1,300 employees quarterly and conduct mandatory neutrality training for each employee annually; and we have a proven Neutrality Code of Conduct. Neustar's proposal will not include a "cure plan" for neutrality. If Neustar is selected, the Industry and FCC will not be forced to evaluate the neutrality of a parent company or set of subcontractors, and there will be no "undue influence" by any constituents of LNP administration. In short, the Industry can proceed with confidence that the neutrality rules will not be diluted under Neustar's tenure.

## LNP Experience

As described in Proposal Section 2.4, Neustar's LNP Expertise, there is no LNP implementation in the world that compares to that of the U.S. and, as such, there is no LNP administration service in the world that compares to the service provided by Neustar. The NPAC/SMS processed over 3.1 Billion transactions since 1998. This number is more than all other centralized LNP database systems in the world combined. We have been a LNP administrator longer than any other vendor in the world, and as such have the Industry's most trusted and knowledgeable staff dedicated to the LNPA service in place today—there will be zero risk in ensuring a competent and capable team is prepared and engaged to support the Industry. Unlike a majority of LNPA implementations internationally, Neustar is not proposing the use of any subcontractors or third-parties to augment our experienced staff.

## Customer Service

The Industry understands the importance of the U.S. LNPA's customer service, making it the most important factor under the Management Criteria in RFP Section 14.1.1.b Evaluation Criteria. Neustar's U.S. LNPA customer service track record is unmatched. As detailed in Proposal Section 2.5, Neustar's Record of Customer Service, Neustar has been rated "Superior" by the Industry since 2009 and we rated a near flawless 3.84 out of 4.0 in 2012 for overall customer satisfaction. During the last five years, we have satisfied the 27-specific U.S. LNPA service level requirements a remarkable 99.94% of the time.

## 2.1 Corporate Experience



### Company Facts

- Neustar serves more than 14,000 customers around the world
- Delaware Corporation, headquartered in Sterling, Virginia
- 17 office locations within the United States; 4 office locations in Europe, Asia, and Central America
- Over 1,300 employees with the majority in the United States
- Founded in 1998
- Publicly traded under the NYSE as NSR

**Data**—Neustar provides real-time information and analytics for almost 7 billion physical and virtual addresses:

- 3.8 billion Global Telephone Numbers
- 2.8 billion Global IP Addresses
- 5.8 million Global Domain Names
- 13.9 million US Business Listings

**Answers**—Neustar provides instantaneous answers to over 30 billion queries from the internet, communications, entertainment, and marketing industries. We answer almost 400 thousand queries every second.

- 18 billion daily DNS query resolutions
- 7 billion daily text messages (US)
- 4 billion daily phone calls (US)
- 3 billion daily geo-location searches
- 2 billion daily on-demand real-time analytic queries

Since our inception, Neustar has been trusted by the FCC and the U.S. telecommunications industry (Industry) to provide neutral, even-handed, and reliable third-party services such as LNP Administration, NANP Administration, National Thousands-block Pooling Administration, and more recently the iTRS Telephone Numbering Directory Administrator.

Over the years, as shown in Exhibit 2.1-1, Neustar has grown from our flagship services to offer a broad range of innovative services, including registry services, managed domain name system (DNS) services, Internet Protocol (IP) services, Internet security services, and Web performance monitoring services. In late 2011 Neustar acquired Targus Information Corporation, or TARGUSinfo. The acquisition of TARGUSinfo, which formed our new Information Services segment, significantly extends our portfolio of services in the real-time information and analytics market.

As discussed below, Neustar operates in three distinct segments: Carrier Services, Enterprise Services, and Information Services. In addition, the remainder of this section describes other attributes that define Neustar and provide value to the Industry including our: Key Corporate Capabilities, Approach to Privacy and Data Security, Industry Involvement, and Corporate Citizenship and Conduct.

## Neustar's Portfolio of Services

Neustar's neutral, third-party stewardship of Industry resources allow organizations to find, connect, and authenticate customers as well as the data they seek.

- North American Numbering Plan Administrator since 1998
- National Thousands-Block Pooling Administrator since 2002
- Local Number Portability Administrator since 1998
- U.S. Common Short Code Administrator since 2003
- iTRS Telephone numbering Directory Administration since 2008
- GSMA Pathfinder Operator since 2008
- U.S. ccTLD Registry Operator since 2001
- .biz TLC Registry Operator since 2000
- DECE UltraViolet™ Digital Locker Operator since 2010

Neustar's policy management and analytics solutions allow companies to optimize management of their corporate services, systems, and data in an on-demand capacity with low up-front costs.

### Neustar Carrier Services



#### Numbering Services

- Local Number Portability Administrator
- North American Numbering Plan Administrator
- National Thousand-Block Pooling Administrator
- iTRS Telephone Numbering Directory Administrator
- LNP Enhanced Analytical Platform
- Intermodal Ported TN Identification Services
- Legal Compliance Services
- Fraud Management
- Port-PS and Number Analyzer



#### Order Management Services

- ASR
- CARE
- E911
- ESR
- ICP
- LIDB/CNAM
- LSR
- WNP
- SOA



#### IP Services

- GSMA Pathfinder
- Multi-Media Interconnect Services (MMIS)

### Neustar Enterprise Services



- Domain Name Registry Services
- DNS Management/Internet Infrastructure Services
- DECE UltraViolet™
- Common Short Codes (CSC)
- NeuSentry

### Neustar Information Services



- Identification Services
- Verification and Analytics Services
- Local Search and Licensed Data Services



126.npac2013

**Exhibit 2.1-1** Neustar is a trusted, neutral provider of real-time information and analytics to the communications, internet, entertainment, advertising, and marketing industries throughout the world.

## Carrier Services

Neustar's customers face increasingly complex technical and operating challenges, particularly as the communications industry makes the transition to an all-IP network. Leveraging our set of unique databases and geographically dispersed data centers, Neustar helps our customers manage this complexity and ensures the seamless connection of their numerous networks while enhancing the capabilities and performance of their infrastructure. Neustar enables our carrier customers to use, exchange, and share critical information such as telephone numbers. We facilitate order management and work flow processing among carriers and allow operators to direct, prioritize, and optimize the addressing and routing of emerging IP communications.

## Numbering Services

Numbering Services includes our role as the United States LNP administrator, our role as the LNP administrator in Canada, as well as our role as the provider of tailored LNP software solutions to the LNP administrators in Taiwan and Brazil (all set forth in Proposal Section 2.4, LNP Expertise). Additionally, Neustar has been the North American Numbering Plan Administrator (NANPA) since 1999, the U.S. Thousands-Block Pooling Administrator (PA) since 2002, and the iTRS Telephone Numbering Directory Administrator since 2008 under contracts with the FCC. These roles are described in Table 2.1-1 along with other Neustar Numbering Services.

Table 2.1-1. Neustar's Numbering Services

Service	Description
Local Number Portability Administrator (LNPA)	Under agreements first executed in 1997, Neustar has served as the LNPA, operating the authoritative NPAC/SMS databases for all regions in the U.S. and Canada. The NPAC/SMS is part of the infrastructure for the communications industry, providing the local number portability that supports the continued convergence of wireline, wireless, voice over Internet protocol (VoIP), and IP communications. Today, the NPAC is the world's largest number portability registry, managing over 600 million telephone numbers for over 2,000 carriers across the U.S. and Canada. Neustar, as the LNPA, earned our <b>highest-ever overall satisfaction rating of 3.84 out of 4.00</b> in the U.S. LNPA Customer Survey Score in 2012.
North American Numbering Plan Administrator (NANPA)	Neustar has served as the North American Numbering Plan Administrator (NANPA) since 1997 pursuant to a contract with the FCC. The NANPA is responsible for the neutral administration of North American Number Plan (NANP) numbering resources, subject to directives from regulatory authorities in countries that share the NANP. NANPA's responsibilities include the assignment of NANP resources, coordination of area code relief planning, and the collection of utilization and forecast data from Service Providers. The FCC has recognized Neustar's superior performance by twice awarding it new contracts, most recently in 2012. Every year, the NANC NOWG produces a detailed performance evaluation of the NANPA. In the most recent evaluation, for the year 2011, the NOWG rated Neustar's performance as NANPA as "EXCEEDED."
National Thousands-Block Pooling Administrator (PA)	Neustar has served as the Thousands-Block Pooling Administrator (National PA) since 2002, pursuant to a contract with the FCC. The National PA performs the day-to-day activities necessary for the assignment and administration of numbering resources in thousands-block, which includes maintaining a system to support all day-to-day and long-term pooling functions. The National PA is also responsible

Service	Description
	for the day-to-day administration and assignment of p-ANIs to wireless and VoIP Service Providers. Every year, the NANC NOWG produces a detailed performance evaluation of the National PA. In the most recent evaluation, for the year 2011, the NOWG rated Neustar's performance as the National PA as "MORE THAN MET."
Internet-based Telecommunications Relay Service (ITRS) Telephone Numbering Directory Administrator	The ITRS Telephone Numbering Directory provides a mapping between the telephone number assigned to hearing or speech impaired persons and the IP addresses of their videophones (for Video Relay Service, or VRS) and the screen names of their IM connections (for IP Relay). The Neustar ITRS Telephone Numbering Directory is based on the ENUM protocol. Under contract with the FCC, Neustar developed and deployed the directory and has operated it since 2008.
Local Number Portability Enhanced Analytical Platform (LEAP)	The LEAP service is designed to facilitate authorized access to portability data for law enforcement, public safety dispatch personnel, and authorized supporting organizations in an environment where time is often of the essence. The service operates via Security-Related Information. It permits qualified customers to submit a telephone number (or a list of up to 100 numbers) and receive a limited subset of NPAC information associated with those numbers, specifically the identity and contact information for the controlling network Service Provider and (if available) for the reseller or alternative Service Provider.
Inter-modal Ported TN Identification Services (IPTN)	Inter-modal porting is one of the key benefits offered to U.S. consumers via the NPAC, and millions of subscribers have taken advantage of it. The IPTN system delivers on a daily basis a comprehensive file of telephone numbers and telephone number ranges that have transferred from fixed line Service Providers to wireless ones, and vice versa. This makes it possible for telemarketers and credit/collections agencies to quickly and reliably provision their systems to maintain compliance with the Telephone Consumer Protections Act (penalties for violations of the TCPA can be over \$11,000 per incident)
Legal Compliance Services	Legal Compliance Services provides cost-effective business solutions that reduce the complexity and mitigate the risk associated with managing a comprehensive legal compliance program. Neustar, as a Trusted Third Party, has a dedicated, specialized area of practice that is staffed with attorneys, paralegals, and certified network engineers to assist or fully manage these mandated services. In addition to working with carriers to ensure compliance with subpoenas for the production of telephone records, Neustar works with carriers to implement a comprehensive CALEA compliance program.
Fraud Management	Fraud Management Services from Neustar helps Service Providers detect several areas of potential fraud in their business, such as: <ul style="list-style-type: none"> <li>• Subscription fraud</li> <li>• Wholesale fraud</li> <li>• Back-office fraud</li> <li>• Bypass fraud</li> <li>• Enterprise fraud</li> <li>• Sales Channel/Dealer fraud</li> </ul>

Service	Description
Port PS and Number Analyzer	<p>Port Power Search (Port PS) is a user friendly, web-based application that provides real-time access to authoritative, Industry telephone number (TN) data and seamless integration with the Pooling Administration for block and code provisioning. Port PS provides a one-step process to query for primary and alternative telephone number Service Provider information.</p> <p>Number Analyzer is a feature of PortPS providing a graphical view of carrier TN inventory, via standard interfaces to the NPAC/SMS, NANPA, and National PA in near real-time so customers may view the most accurate and up-to-date information available. For example, customers can begin by viewing their number inventory by NPAC region and then drill down to view details including:</p> <ul style="list-style-type: none"> <li>• Telephone numbers lost and gained due to porting and pooling</li> <li>• Inventory by switch to identify load balancing needs</li> <li>• Utilization thresholds for ordering or donating</li> </ul>

**Order Management Services**

Neustar's Order Management Services (OMS) includes all operations necessary to manage number port activity. The process starts with an assessment of whether the change requires the updating of the NPAC, directory services, and/or E911. Neustar has automated nearly all of the steps required of carriers to port a telephone number. The entire process includes managing the physical interconnectivity among the networks and communications among the carriers. Neustar offers a turn-key, end-to-end porting solution to our customers. Our unique workflow and transaction processing databases and systems (described in the Table 2.1-2) enable Service Providers to exchange essential operational data in a secured manner.

**Table 2.1-2. Neustar's Order Management Services**

Service	Description
Access Service Request (ASR)	<p>Neustar provides an integrated solution for ordering access from multiple providers. Through a single Web-based interface, ASR helps Service Providers expedite customer provisioning or network capacity expansion through an "e-bonding" process using Industry-accepted standards. ASR eliminates the need for one-to-one interfaces across trading partners to help lower operating and administrative costs.</p>
Customer Account Record Exchange (CARE)	<p>Neustar's CARE clearinghouse capabilities support all requirements set by the Ordering and Billing Forum (OBF) of the Alliance for Telecommunications Industry Solutions (ATIS). Neustar's CARE platform enables automated, timely exchange of records between local exchange carriers (LECs) as well as interexchange carriers (IXCs).</p>
Enhanced 911 (E911)	<p>Neustar's E911 module features an interface that allows continuous updates to the Automatic Location Identification (ALI) database. The local public safety answering point (PSAP) queries the ALI using the caller's telephone number. The PSAP is able to quickly identify the geographic location of the caller and accurately notify first responders.</p>

Service	Description
Enhanced Service Request (ESR)	Neustar's ESR enables Emerging Service Providers (ESPs) and CLECs to manage subscriber expectations, process customer orders and generate revenue through automation, order uniformity and business rule validation. ESR allows ESPs to port numbers for their customers in a well-defined process with end-to-end flow-through provisioning from CLECs.
Line Information Database/Calling Name (LIDB/CNAM)	<p>Neustar's LIDB/CNAM module provides gateways to various LIDB and CNAM databases, and supports the following subscriber record requests:</p> <ul style="list-style-type: none"> <li>• Calling Card (insert or change a calling card record)</li> <li>• LIDB (insert, change or delete a line number record)</li> <li>• CNAM (insert, change or delete a calling name)</li> </ul> <p>The LIDB contains subscriber information such as a service profile, 10-digit line numbers, Service Provider ID, equipment indicator, and billing specifications. The CNAM databases enable carriers to provision the calling name associated with a particular line number.</p>
Local Service Request (LSR)	Neustar's LSR capabilities streamline the process whenever a Service Provider interfaces with an incumbent local exchange carrier (ILEC) to set up services for their customers. In addition to reducing change management expense, operational efficiencies are realized as provisioning personnel are able to submit and manage all LSR orders to all ILECs through a single automated interface.
Wireless Number Portability (WNP)	Neustar's WNP capabilities permit Wireless Service Providers to exchange wireless-to-wireless port requests, intermodal port requests, and interact with the NPAC while complying with industry standards. WNP is provided within the framework of Neustar's clearinghouse to allow Service Providers to turn up accounts quickly with cost-effective, standards-compliant automated porting processes. This solution provides an end-to-end wireless solution by supporting ICP, SOA and Intermodal type transactions.
Intercarrier Communications Process (ICP)	<p>Neustar's ICP is an integral part of the company's Wireless Number Portability (WNP) Clearinghouse model. The ICP was designed to automate all wireless-to-wireless port request transactions between Wireless Service Providers. Transactions are sent to Wireless Service Providers through a single, integrated service, which includes the following ICP transactions:</p> <ul style="list-style-type: none"> <li>• Wireless Port Request (WPR)</li> <li>• Wireless Port Request Response (WPRR)</li> <li>• Supplemental Port Request (SPR)</li> </ul>
Service Order Administration (SOA)	Neustar's SOA interfaces with the NPAC to allow Service Providers to complete any number porting requests. When using SOA within Neustar's clearinghouse, Service Providers realize the benefits of an end-to-end porting process – from LSR for wireline number porting and ICP for wireless number porting requests – integrated with SOA.
Intermodal Manager (IMM)	Neustar is the only provider of automated Intermodal porting services in the US. Our unique solution is designed to enable Wireless and Wireline Service Providers to port amongst each other regardless of the Service Provider type. The Intermodal Manager (IMM) solution interfaces with Wireline and Wireless Service Providers in the port request format they accept and adhere to. The Wireless ICP

Service	Description
	requests will be enriched and translated to LSR format to the exact specifications acceptable by Wireline Service Providers. The Wireline LSR requests are also enriched and translated to ICP Wireless requests and then sent to Wireless Service Providers. ICP and LSR responses are all translated back to the proper format before sending to the originating party. All LSR and ICP type transactions are supported in this solution.

**IP Services**

Neustar provides scalable IP services to Service Providers that allow them to manage access for the routing of IP communications, such as multimedia messaging service. Our solutions, described in the Table 2.1-3, solve the complexity of mapping a telephone number to an IP address for accurate and reliable routing to a carrier's network. We also enable direct network-to-network peering between Service Providers for voice, video and content services.

**Table 2.1-3. Neustar's IP Services**

Service	Description
GSMA Pathfinder	The transition from the voice-centric circuit switched world to an all-Internet Protocol (IP) environment supporting voice and data brings both opportunities and challenges. As services migrate to a converged infrastructure, operators require solutions that support route identification and deliver interoperability for all new services. The Global System Mobile Association (GSMA) and Neustar have been working with leading operators to provide a standards-based solution to this problem. This solution is a Number Translation Service called PathFinder, operated by Neustar on behalf of the GSMA. The service facilitates IP inter-operability by translating telephone numbers to IP-based addresses. Based on Carrier ENUM (E.164 Number Mapping), PathFinder is available to mobile operators, fixed network operators, and related Service Providers. PathFinder is provided as an off-the-shelf managed service, inter-operable on a global basis, providing all the facilities and features necessary to implement an operator's interconnect policies.
Multimedia Interconnect Services (MMIS)	Neustar's MMIS offers query-based access for real-time routing of Multimedia Messaging Service (MMS) traffic. This service provides the telephone to uniform resource locator (TN-to-URL) mapping for reliable message termination between Service Providers. The subscriber's application queries MMIS, which responds with terminating Service Provider information.

**Neustar Enterprise Services**

We provide Internet infrastructure services (described in Table 2.1-4) that our customers use in order to direct, prioritize and manage Internet traffic. In addition, enterprise customers rely on our services to optimize their Website performance, including protecting against malicious traffic. Enterprises use our broad infrastructure and unique datasets to identify the location of their online customers for a variety of purposes, including fraud prevention and marketing. Our registry services provide reliable, fair and secured access used for resolving top-level domain name Internet queries. We also operate the authoritative Common Short Codes registry on behalf of the U.S. wireless Industry.

Table 2.1-4. Neustar's Enterprise Services

Service	Description
Domain Name Registry Services	<p>Neustar operates the authoritative registries of Internet domain names for the .BIZ, .US, .CO, .TEL, and .TRAVEL top-level domains. In mid-2012, Neustar was selected as the registry services provider for 356 new generic Top-Level domains (gTLDs), under consideration by ICANN. Additionally, Neustar has been selected by the City of New York as the registry provider to manage the application process and operate the .NYC gTLD. All Internet communications routing to any of these domains must query a copy of our directory to ensure that the communication is routed to the appropriate destination. We also provide international registry gateways for China's .CN and Taiwan's .TW country-code top-level domains.</p>
Internet Infrastructure Services	<p>Neustar provides an innovative suite of network services for its enterprise customers. UltraDNS® is the industry-leading managed DNS and traffic management service. Built on a global platform, UltraDNS® directs, prioritizes and manages Internet traffic, and finds and resolves Internet queries and top-level domains on behalf of its enterprise customers. Neustar provides a suite of DNS services to our enterprise customers built on a global directory platform. These services play a key role in directing and managing Internet traffic flow, resolving Internet queries, providing security protection against Internet breaches called Distributed Denial of Service attacks, providing location services used to enhance fraud prevention and online marketing, and monitoring, testing and measuring the performance of websites and networks. Webmetrics monitoring and load testing provides comprehensive reporting and data on the user experience of a web property including unique views of ecosystems and web mashups.</p>
DECE UltraViolet™	<p>The UltraViolet™ media platform allows consumers to "buy once, play anywhere" convenience for all their digital entertainment contents. Neustar operates the digital content authentication directory on behalf of DECE UltraViolet™ ecosystem.</p>
Common Short Codes (CSC)	<p>Neustar provides directory services for the 5-digit and 6-digit number strings used for all U.S. Common Short Codes (CSC), which is part of the short messaging service relied upon by the U.S. wireless industry. CSCs are short numeric codes to which text messages can be sent from a mobile phone when the subscriber's wireless carrier participates in the CSC registry. A content provider can lease a CSC online to tap the considerable potential of the mobile market with targeted campaigns and applications, including voting, polling, contests and sweepstakes, coupon redemption, gaming, database queries, and more</p>
NeuSentry	<p>NeuSentry is a new, innovative network security tool. With NeuSentry, our experts work with customers to identify physical and electronic security events that affect an organization's risk profile. Specifically, we:</p> <ul style="list-style-type: none"> <li>• Identify a set of likely signs, symptoms and trace evidence markers that indicate the occurrence of a security threat/event</li> <li>• Customize Neustar's Global Threat Monitoring Platform™ (GTMP™) to alarm when any event within a customer's profile is detected by our sensor network</li> <li>• Notify customers when breaches occur in real-time, to minimize loss due to attack</li> <li>• Work with our customers, after the event, to address the severity of the attack, the damages involved, and the identity of the attackers</li> <li>• Adapt the process to improve the identification of evidence markers</li> </ul>

## Neustar Information Services

Neustar's Information Services segment provides a broad portfolio of real-time information and analytics services that enable clients to:

1. Identify incoming customer contacts, verify customer-provided contact information, and customize the communications with customers and prospective customers/prospects—all in real time; and
2. Understand and respond to customer interests and preferences based on insights derived from large groups of similar consumers.

We are one of the largest non-carrier providers of Caller ID services, and provide a comprehensive market analytics platform that enables clients to access and apply rich insights about customers and prospects derived from hundreds of reliable sources for privacy-friendly real-time interactive marketing initiatives. Additionally, our business listings product suite provides local businesses and local search platforms with a single, trusted source of verified business listings for local searches. Our online audience marketing product suite enables online advertisers to display relevant advertisements to specific audiences without compromising user privacy, increasing the effectiveness of online advertising and delivering a more useful online experience for consumers. Neustar has three distinct product suites within our Information Services business as described in Table 2.1-5.

Table 2.1-5. Neustar's Information Services

Neustar Information Services	Description
Identification Services	Our Identification Services product suite provides Caller ID services to carriers in the U.S. and real-time identification and location services to over 1,000 businesses in the U.S. across multiple industries. Our location service enables clients to match a 10-digit phone number to a latitude and longitude location, and is used for a number of applications including intelligent site planning, evaluating the market potential for retail locations, and web-based location lookup.
Verification and Analytics Services	Our Verification and Analytics Services product suite provides lead verification services that allow clients to validate customer data, enhance leads, and understand the likelihood that a particular lead will convert. This lead verification application enables customers to maximize their return on inbound telephone and web leads, identify the prospects that are most likely to become loyal customers, or for current customers, select and present the most effective up-sell offer.
Local Search and Licensed Data Services	Neustar's Local Search and Licensed Data Services product suite provides an online local business listing identity management solution that serves local search platforms, national brands, authorized channel partners and local businesses. This service gives businesses and channel partners essential tools to verify, enhance and manage the identity of local business listings on local search platforms across the web, and offers search platforms an accurate, complete and up-to-date database of local business listings for online publishing.



## Neustar’s Key Corporate Capabilities

Neustar’s service offerings, regardless of segment, are customer-centered and founded on four key components:

1. **Reliability**—Neustar’s service offerings depend on complex technology configured to deliver high reliability consistent with stringent Industry and customer standards. We have made a commitment to our customers to deliver high quality services that meet or exceed numerous measured service level requirements, such as system availability, response times for help desk inquiries, and billing accuracy.
2. **Scalability**—By design, Neustar’s infrastructure enables capacity and functionality expansion without service interruption or quality of service degradation.
3. **Neutrality**—Neustar provides its numbering administration services in a competitively neutral way to ensure no Service Provider or Industry segment is favored over any other. Our databases and capabilities provide competing entities with fair, equal, and secure access to essential shared resources. Neustar’s performance with respect to neutrality and safeguarding customer and subscriber data are independently audited on a regular basis.
4. **Trustworthiness**—The data Neustar collects is proprietary to our customers. Accordingly, we have implemented appropriate procedures and systems to protect the privacy and security of customer data, restrict access to Neustar IT systems, and protect the integrity of its databases.

In addition to our demonstrated financial and operational stability as detailed in Proposal Section 2.2, Neustar’s Financial and Operational Stability, and our proven neutrality as detailed in Proposal Section 2.3, Neustar’s Neutrality, we have built and grown a large set of key, core corporate capabilities as shown in Table 2.1-6. Many of these corporate capabilities tie directly to the evaluation criteria set forth in the RFP.

**Table 2.1-6. Neustar’s Key Corporate Capabilities**

Corporate Capability	Neustar’s Experience
Meet schedule requirements and manage contract costs	<ul style="list-style-type: none"> <li>• NPAC/SMS SOWs (including development, quality assurance, deployment, and Service Provider certifications have been subject to Industry schedule and cost audits</li> <li>• All NPAC/SMS SOWs have been completed to specification and on time</li> </ul>
Provide full financial and operational reporting and insight	<ul style="list-style-type: none"> <li>• Neustar publishes and provides an Annual Report to the FCC and NANC, and remains in constant contact with both organizations regarding ongoing performance and other activities</li> <li>• Neustar provides a written report in conjunction with an oral presentation at every NANC meeting and responds to questions</li> <li>• Neustar meets monthly with the NANC’s NOWG to review its performance measurements</li> <li>• We have provided the 2011 Neustar Annual Report and the 2012 10-K</li> </ul>
Develop and implement escalation procedures	<ul style="list-style-type: none"> <li>• Effective escalation procedures are in place for the NPAC/SMS</li> <li>• NPAC/SMS reports into the Senior Vice President, Carrier Services</li> <li>• Short, clear lines of escalation ensure timely address of issues as they arise</li> </ul>

Corporate Capability	Neustar's Experience
Survey end users to gain feedback on help desk and user experience	<ul style="list-style-type: none"> <li>• Annual NPAC Customer Survey administered by independent third party</li> <li>• Distributed to all NPAC Users</li> <li>• Designed to assess neutrality, responsiveness, Industry knowledge, urgency, and accuracy of all NPAC/SMS customer touchpoints</li> </ul>
Administration of complex, vital U.S. public resources	<ul style="list-style-type: none"> <li>• NANP Administration</li> <li>• National Thousands Block Pooling Administration</li> <li>• .US ccTLD Registry</li> </ul>
Facilitation of controlled, systematic evolution, enhancement, and expansion of Industry functions	<ul style="list-style-type: none"> <li>• Neustar performs the change management administration function for the NPAC/SMS on behalf of the communications Industry</li> <li>• Neustar facilitated the transition of state number pooling trials to a national database, focusing on a systematic evolution allowing for growth and future enhancements</li> <li>• Neustar works closely with Industry and the FCC to develop enhancements to the existing NANPA process, including expansion of current functions</li> </ul>
Experience designing, developing, deploying, and supporting robust systems and databases	<ul style="list-style-type: none"> <li>• Neustar designed, developed, deployed, and expanded the NPAC/SMS database to its current support of more than 620 million telephone numbers.</li> <li>• Neustar designed, developed, deployed, and support NANPA Administration System (NAS).</li> <li>• Neustar designed, developed, deployed, enhanced, and support the Pooling Administration System (PAS).</li> <li>• Neustar designed and built the next generation DNS architecture for registries such as .US and .biz.</li> </ul>
Manage a high-availability system to contractual service levels	<ul style="list-style-type: none"> <li>• The NPAC/SMS is subject to 27 contractual service level requirements, developed jointly with the industry, which are reported on monthly</li> <li>• The iTRS Telephone Numbering Directory is required to maintain 99.999% availability for both its provisioning and its query functions</li> <li>• The UltraDNS service and all Neustar's TLD registries carry service level requirements of 100% uptime – zero planned or unplanned outages permitted</li> <li>• The .biz registry has SLAs with several major channel partners covering system downtime and system performance measures</li> </ul>
Strong working relationships and communications with a wide-spectrum of organizations, customers, and stakeholders	<ul style="list-style-type: none"> <li>• Neustar actively participates in various Industry forums, including LNPA WG, NOWG, Industry Numbering Committee (INC), Internet Engineering Task Force (IETF), Internet Corporation of Assigned Names and Numbers (ICANN), and International Telecommunications Union (ITU)</li> <li>• Neustar provides assistance to both the communications Industry and regulators in an effort to resolve difficulties in the area of number assignment, reporting, etc.</li> <li>• Neustar provides the Industry Change Management Function for the LNPA</li> </ul>
Facilitation of progress in a competitive environment with regulatory oversight	<ul style="list-style-type: none"> <li>• Neustar acted as interim pooling administrator in several states prior to being selected as National Pooling Administrator.</li> <li>• Neustar facilitates NPA relief planning meetings, resulting in a relief plan which meets the needs of the Industry and the regulators.</li> <li>• Neustar provides objective information and assistance to the LNPA WG in an effort to resolve issues facing the entire communications Industry.</li> </ul>

Corporate Capability	Neustar's Experience
Ability to address long-term resource planning issues	<ul style="list-style-type: none"> <li>• Developed Number Resource Utilization Forecasting (NRUF) tool, ensuring appropriate detailed carrier information is collected, stored, analyzed, and properly distributed to appropriate regulatory authorities</li> <li>• Work closely with INC, NANC, and LNPA WG to ensure that long term Number Resource Optimization needs will continue to be achieved.</li> </ul>
Experience in building scalable databases that ensure security and privacy of customer data	<ul style="list-style-type: none"> <li>• Neustar developed, deployed, and maintains the Number Portability Administration Center, which contains routing information for ported and pooled telephone numbers in the U.S. and Canada.</li> <li>• Neustar developed, deployed, and supports the Customer Account Record Exchange database, which contains highly sensitive proprietary Service Provider information.</li> </ul>
Ability to understand, administer, and deploy services that implement telecommunications and Internet policy	<ul style="list-style-type: none"> <li>• Neustar has an in-depth understanding of all federal and state policy issues regarding number administration, including the requirements developed by the Industry that are seen to be the guidelines under which the LNPA, NANPA, and the PA operate; all services are fully compliant with all regulatory and Industry mandates</li> <li>• Neustar's experience in the policy-rich communications regulatory environment provides it with significant insight into policy identification and coordination of Internet policy</li> <li>• Neustar is active in ICANN, the IETF, and other Internet-related policy and standards bodies. Neustar has a staff of experts on Internet policy and technical matters. Neustar policy and legal experts participate heavily in ICANN activities</li> </ul>

## Neustar's Approach to Privacy and Data Security: Coordinated, Comprehensive, Built-In

Neustar's corporate heritage is grounded in the principle of neutrality, the building blocks of which are trust, privacy, and security. We understood from the very outset that the U.S. telecommunications Industry would not assign us responsibility for managing their critical assets (i.e. telephone number inventory) without absolute confidence that Neustar would aggressively defend those assets from unauthorized use, access, disclosure, or alteration. Neustar's goal, from its earliest days, is to be the relentlessly neutral, unassailably trustworthy, and demonstrably reliable provider of best-in-breed services and technology fueled by some of a provider's most important assets—confidential and competitively sensitive business information.

We know privacy and security safeguards must be built into—not added onto—everything we do in order to achieve this goal. ensure that the information we receive as the LNP administrator remains the confidential information of the providing users, and prevent use of that data other than for the performance of our obligations as the NPAC administrator and as permitted by our User Agreements. Moreover, we believe that privacy and security are but two legs of a three legged stool that must include data governance.

In recognition of the increasing complex issues surrounding data privacy and security, and the interdependence of these concepts, Neustar formally adopted an enterprise-wide "privacy and security by design" approach to safeguard data entrusted to us by our customers, and two individuals with extraordinary expertise and experience were brought in to spearhead this approach.

# CONFIDENTIAL

We have implemented, and continuously update, strict data privacy security policies throughout the company, including policies and practices applicable specifically to NPAC data that meet or exceed the administrative, technical, and physical security requirements of the Master Agreement. Compliance with these requirements is monitored and auditable under the terms of the Master Agreement, and the NPAC infrastructure is subject to an annual security assessment. User Data is, of course, segregated from data used by Neustar in connection with other services, and we have appointed both business and technical "data stewards" for that data. For example, <sup>CONFIDENTIAL</sup> are business and technical data stewards, respectively, for the U.S. NPAC. Access is restricted to employees with a "need-to-know" for purposes of providing services under the Master Agreement and/or User Agreements who have received appropriate training to ensure adherence to the requirements of those agreements.

Controls are further ensured by the company's data governance procedures, which require the Chief Privacy Officer and Deputy General Counsel to review and approve (or disapprove) all data access requests, and to maintain a running log of the disposition of all access requests. In conducting these reviews, the Chief Privacy Officer speaks directly with relevant data stewards and lawyers responsible for the Master Agreement and User Agreement.

The results of our compliance monitoring program confirm the company's adherence to the privacy and security controls in place to protect NPAC data. For example, Neustar undertakes an annual audit of the security of IT Operations for the NPAC application. The annual Neutrality Audit reviews compliance with our obligation to limit

Users access to their own data. As part of Neustar's Sarbanes-Oxley obligations, we review NPAC access, change management procedures, and computer operations controls.

Neustar is committed to continuous improvement and best-practices adherence, and provides Industry leadership as an active member of the Network Advertising Initiative (NAI) and the Digital Advertising Alliance (DAA).

## Neustar's Industry Involvement

Neustar is committed to being actively involved in the industries we serve. We chair and co-chair several Industry forums and we are regular contributors, offering whitepapers and other submissions to several different working groups and committees. We strive to be thought leaders in the areas of our expertise and we take that role seriously. We know that a high degree of trust from our customers is required for us to be successful in working with the Industry to expand ideas in a professional transparent manner. Neustar is an active participant in the following forums, associations, and organizations:

- Alliance for Telecommunications Industry Solutions (ATIS)
- CTIA—The Wireless Association (CTIA)
- Common Interest Group for Routing and Rating (CIGRR)
- Communications Sector Coordinating Council (CSCC)
- Competitive Communications Association (COMPTEL)
- Emergency Services Interoperability Forum (ESIF)
- Federal Communications Bar Association (FCBA)
- Future of Numbering (FON) Working Group
- Future of Privacy Forum
- Global System for Mobile communications Association (GSMA)
- GSMA Embedded Mobile Project
- Industry Numbering Committee (INC)
- Information Technology Sector Co-Ordinating Council
- International Telecommunication Union (ITU)
- Internet Engineering Task Force (IETF)
- Kantara Initiative
- Local Number Portability Administration Working Group (LNPA WG)
- Local Ordering Sub-Committee, OBF
- Mid American Regulatory Commissioners
- Mobile Marketing Association (MMA)
- Murray State University Center for Telecommunications Systems Management
- National Association of Regulatory Utility Commissioners (NARUC)
- National Cable and Telecommunications Association (NCTA)
- National Institute of Standards and Technology Smart Grid Interoperability Standards (NIST SGIP)
- National Telecommunications Cooperative Association (NTCA)
- National Security Telecommunications Advisory Committee (NSTAC)
- New England Conference of Public Utility Commissioners
- North American Numbering Council (NANC)
- Numbering Oversight Working Group (NOWG)
- Open Mobile Alliance (OMA)
- Ordering and Billing Forum (OBF)
- South Eastern Association of Regulatory Utility Commissioners
- Tech America
- Telecommunications Risk Management Association (TRMA)
- Third Generation Partnership Project (3GPP)
- United States International Telecommunication Union Association (USITUA)
- USTelecom
- Wireless Sub-Committee, OBF

We know that special care and conduct are required when being a thought leader while at the same time being a neutral, third-party administrator of an Industry-wide service like the U.S. LNPA. For example, Neustar has never, and would never, sponsor a change order at an Industry forum like the NANC LNPA Working Group, get the Industry to expend considerable resources to define, refine, and work the change order, and simultaneously seek a patent based on that change order. Doing so could potentially prevent the Industry from implementing the subject matter of the change order covered by the patent or enable the vendor doing so to monetize the change order later. Companies that do this just do not understand the conduct, the trustworthiness and, particularly, the neutrality required of the U.S. LNPA.

## Neustar's Corporate Citizenship and Conduct

We will remain worthy of the Industry's trust, a particularly important qualification for an entity providing neutral third-party services. In the LNPA Vendor Qualification document, the Industry requests information from respondents, and any of their proposed subcontractors, with respect to pending lawsuits, contract terminations, past performance on contracts, and current contract references, all of which speak to a respondent's reputation. In Neustar's responses to these questions, the Industry will find an outstanding record. Neustar is proud to say that it is not our practice to sue our customers. As a U.S. company, we respect and abide by U.S. law. We have never been fined by the U.S. government. We do not do business with, or in, foreign countries like Iran, Cuba, or Syria that are under sanctions from the U.S. government. During the next contract term and beyond, Neustar is committed to continue to be a good corporate partner and citizen to the communications Industry and all of our current and prospective customers.

Additionally, Neustar recognizes it is our responsibility, as a good corporate citizen, to help enrich our surrounding communities in a way that leverages our experience as a technology leader. Through successful community initiatives such as the My Digital Life program, which teaches middle school students digital literacy and online safety and excites children about career opportunities in Science, Technology, Engineering, and Math (STEM) fields, Neustar can help prepare an innovative, competitive workforce by getting children interested in these subjects. To date, approximately 23,000 students are participating in the My Digital Life program in more than 220 schools. Neustar's CEO, Lisa Hook, is a passionate advocate for STEM education. She has participated in many programs promoting these fields, authored editorials encouraging the participation of her peers, and participated on a Congressional panel focused on the importance of STEM education to America's job growth and economic recovery. Also, through the leadership of Neustar's CTO, Mark Bregman, the company actively participates in the Anita Borg Institute's annual "Grace Hopper Celebration" event, which supports and promotes the advancement of women in technology.

Just as we believe we have a responsibility to help improve the STEM educational opportunities and to be an environmentally sound neighbor, we believe it is vital to support the relationship between our employees and the broader communities we live in. We offer each of our full-time employees one paid day off each year to volunteer for non-profit and community organizations. In effect, we allow our employees to contribute up to 10,000 hours of paid volunteer time each year.

We also support higher education initiatives that help students further their degrees with real-world experience. In the spring of 2012, Neustar Labs, our research and development arm, established the Neustar Innovation Center at the University of Illinois, Champaign-Urbana, one of the leading computer science schools in the country. Neustar offers internships at the Center, where students research and develop new solutions to real business problems, giving them valuable experience they can apply to future careers. In Kentucky, where we have a major operations center, we are actively working to support universities' engineering programs to help develop a strong pipeline of technical talent. In 2012, we hired our first interns from area colleges and plan to continue offering training opportunities in that community.

Neustar sponsored the CyberWatch Mid-Atlantic Collegiate Cyber Defense (CCDC), competition, where students from regional colleges try to protect networks that a team of "hackers," or security professionals from Neustar and other companies, attempt to compromise. We also participated in The George Washington University's Teachers in Industry Project, which provides middle and high school teachers the opportunity to experience the work environment for which they are preparing their students. This has led us to offer four-day "externships" to STEM teachers at our Security-Related Information campus.

Neustar is an enthusiastic supporter of Yearup!, an intensive training program that provides low-income young adults, ages 18-24, with a combination of hands-on skills development, college credits, and corporate internships—particularly in the technology sector. We have sponsored internships with a number of them becoming full-time Neustar employees.

Neustar also has significant environmental conservation initiatives in place and recently received LEED certification by the U.S. Green Building Council (U.S.GBC) in recognition of Neustar's commitment to managing its energy consumption, water efficiency and material use during the construction process of our headquarters in Information Altered to. We continue to work toward reducing the amount of energy consumed in our data centers through the incorporation of many eco-friendly systems, such as air flow controls and energy-efficient servers, and Neustar sites around the world have numerous recycling and conservation programs in place, including: traditional recycling of paper, glass, aluminum, and plastics; a paperless payroll option for employees; and GreenPrint to reduce paper consumption.

## Conclusion

In conclusion, Neustar, as a corporation, offers the Industry:

- Unmatched credentials as a neutral, third-party services partner for not only the communications Industry but also the internet industry
- Proven core capabilities aligned with evaluation criteria set forth in the RFP
- Enterprise-wide "privacy and security by design" approach to safeguard data entrusted to us by our customers
- Active participation in Industry fora
- Strong community involvement that benefits the industries we serve and the communities we operate in.

## 2.2 Neustar's Financial and Operational Stability

---



### Why Neustar

- Financially strong with growing revenues, cash balances, and earnings per share
  - Stable, with only one ownership change since incorporation in 1998 — going public
  - Publicly traded company with CFO attestation/certification that provides superior financial transparency
  - Not proposing a special-purpose company, a newly formed company, or a wholly owned subsidiary; thereby providing an unclouded picture of our financial and operational stability
  - U.S. company respecting and adhering to U.S. laws and regulations
- 

The Industry requires prospective bidders to provide three-years worth of audited financial statements and annual reports in their proposals, explain their financial position, and provide the same financial information for any subcontractors.

Neustar posits that these are minimum requirements for prospective bidders. We have included the required information (as an attachment to VQS Section 3.2, Financial Responsibility and Stability) and in the remainder of this section, will more precisely describe our financial position. We understand that audited financial statements and annual reports do provide some measure to assess whether an entity has the financial resources to serve as the LNPA for the next term. cursory review of the requested materials can provide some insight into the financial structure of a company; however, only a deeper inspection can reveal the precarious position of a company which otherwise appears fiscally sound. For example, prior to 2000, Industry professionals would not have predicted that Worldcom, Global Crossing, Adelphia Communications, or Nortel would all go bankrupt. Few financial professionals would have predicted that Lehman Brothers, Chrysler, and General Motors would go bankrupt and that over 400 U.S. banks would fail between 2008 and 2011 after only 25 banks had failed in the previous 7 years.

Neustar the parent, not a wholly owned subsidiary of Neustar, serves as the current U.S. LNPA. The financials we state and provide are our own and are not dependent on a disconnected parent company. Additionally, the financial reports we provide adhere to strict laws with respect to publicly traded companies in the U.S. as discussed below.

Respondents who operate as wholly owned subsidiaries may be beholden to their corporate parents for a number of items; demonstration of financial strength, approvals of strategic and operational decisions, and general support of business plans. On the surface, wholly owned subsidiaries may appear to be financially strong based on the financial strength of their parent company. However, to allow for deeper inspection, a wholly owned subsidiary must provide a detailed description of not just its own financial condition but also that of its parent company. In addition, a wholly owned subsidiary must provide detailed budgets and various financial guarantees from its corporate parent so the Industry can eliminate any concerns about the respondent's financial stability.

Likewise, financial statements of private companies can prove to be a challenge when conducting a similar assessment. Generally, privately held companies have less comprehensive reporting requirements for transparency than do publicly traded companies. Additionally, private companies are not subject to regulations like Sarbanes-Oxley and, typically, do not have to operate under the financial rigors and controls. For example, privately held companies in the United States are generally not required to publicly disclose their financial statements. Private companies may make decisions to benefit only a small number of owners/shareholders while leaving the company at risk. At minimum, respondents that operate as privately held entities must provide financial reports and disclosures that are at par with those provided by public companies.

Partnerships, like joint ventures, can prove to be problematic as well; particularly partnerships or entities formed just to bid on a specific project, program, or service. These types of ventures are known as special purpose vehicles or special purpose entities. Some non-neutral bidders may use this approach to create an entity that appears to be free of any neutrality concerns, but in attempting to cure neutrality concerns, they may end up with one that has no discernible financial track record or substance.

Since our inception in 1998, Neustar has understood that financial stability is a vital pillar for providing LNPA services to the Industry. Our strong and stable financial position and our corporate commitment to serve as the U.S. LNPA has allowed us to provide consistent and high levels of LNPA customer service during trying economic times.

As further detailed below, Neustar does not propose the use of any subcontractors to deliver U.S. LNPA services. Respondents that propose the use of subcontractors make it difficult, if not impossible, for the Industry to rely upon the financial disclosures offered by the primary vendor. Neustar is a U.S.-based company and is not foreign-based or foreign-controlled. Foreign-based/foreign-controlled companies have several inherent drawbacks, being subject to different financial reporting requirements, different corporate ethics, and different laws.

### **Neustar's Financial Performance**

Neustar has been a public company since 2005 and has undergone only one change in ownership since 1998—going public. Neustar is a financially strong and stable company with annual revenue growing from \$242M in 2005 to \$831M in 2012. Likewise, Neustar's annual free cash flow has almost quadrupled going from \$48M to \$251M during the same time frame.

Neustar's principal source of liquidity is cash provided by our operating activities. Neustar's business segments have strong fundamentals and generate enough cash to meet all our obligations and make all necessary investments in our technology platforms.

Neustar manages its business very conservatively with specific focus on long-term viability and financial stability. We have an exceptionally strong balance sheet, particularly in regard to working capital. As of December 31, 2012, our Working Capital (current assets minus current liabilities) equaled \$368.3 million, including \$343.9 million of liquid cash, cash equivalents, and short term investments. Financial ratios for financial stability exceed common performance benchmarks—our current ratio (ratio of current assets to current liabilities) of 3.3 and our quick ratio (ratio of liquid assets to current liabilities) of 3.0 exceed typical benchmarks for these ratios of 2.0 and 1.0, respectively.

In addition to strong liquidity, our debt to equity ratio of 0.9 is favorable when compared against a common benchmark of 1.5. Our net debt to equity ratio (debt minus cash and cash equivalents versus equity), which indicates the relative proportion of shareholders' equity and debt used to finance a company's assets, is under a benchmark of 1.0 at 0.38.

### **Neustar's Revenue Diversification**

Neustar's commitment is to improve U.S. LNPA services continually while judiciously taking advantage of strategic opportunities to diversify revenue and maximize overall long-term viability. During the last several years, Neustar has successfully diversified its business without losing sight of our role as the U.S. LNPA.

Over the years, we've diversified our services portfolio and now offer a broad range of innovative services, including registry services, managed DNS services, IP services, fixed IP geolocation services, Internet security services, caller ID services, Web performance monitoring services, and real-time information and analytics services. This has been accomplished through acquisitions of strategic assets such as Neustar Information Services (formerly TARGUS info), as well as organic growth.

It is also extremely important to note that our revenue growth has been entirely from "neutral" businesses. In fact, neutrality is a foremost investment/business review criteria for Neustar. We never will enter or acquire a business that makes us non-neutral and jeopardizes our role as the U.S. LNPA. Over the past 15 years, as discussed below in Proposal Section 2.3, Neustar's Neutrality, we have passed on business opportunities and acquisitions that would possibly have added annually hundreds of millions to our revenue annually and significantly increased shareholder value. We have never lost sight of the fact that the largest source of our strength and track record comes from our work as the U.S. LNPA.

### **Neustar's Credit Facilities**

On January 22, 2013, we entered into a credit facility that provided for a \$325 million senior secured term loan facility, or 2013 Term Facility, and a \$200 million senior secured revolving credit facility, or the 2013 Revolving Facility, and together with the 2013 Term Facility, the 2013 Credit Facilities. In addition, we closed an offering of \$300 million aggregate principal amount of 4.50% senior notes, or Notes. We used the proceeds received from the 2013 Term Facility and Notes to repay our outstanding principal borrowings of \$592.5 million under the 2011 Term Facility. Our 2011 Credit Facilities, which we used to purchase TARGUSinfo, were terminated in connection with this refinancing event.

Our ability to raise debt on favorable terms in a weak economic environment speaks strongly of the confidence placed on us by the financial community, while our willingness to purchase strategic assets at a time when asset prices and interest rates are at their lowest levels in many years speaks to the business acumen and strategic vision of our management team and Board of Directors.

Regardless of whether Neustar is in the process of diversifying our revenue or seeking to expand our access to credit or debt, adhering to Neutrality Requirements is of paramount importance. As such, specific provisions are included in our debt instruments to ensure no TSP can ever hold a majority of our debt. These debt documents are filed with the SEC and are publicly available.

### **Neustar's Public Financial Reporting and Transparency**

As a publicly held company since 2005, Neustar is fully compliant with all required financial reporting and disclosures required by the SEC and in accordance with U.S. Generally Accepted Accounting Principles (GAAP). The company has maintained effective disclosure controls and internal control over financial reporting based on the criteria established in Internal Control-Integrated Framework issued by the Committee of Sponsoring Organizations of the Treadway Commission. Further, we have designed accounting, IT and operational procedures that exceed the Sarbanes-Oxley requirements. Neustar has maintained a rigorous accounting and reporting practice with regular reviews by the company's Board of Director's Audit Committee and its registered public accounting firm, Ernst & Young. The company's approach to financial reporting, public disclosure and internal control is evidenced by the fact that the company has not disclosed any significant deficiencies or material weaknesses in internal control over financial reporting, nor has the company disclosed errors in its financial statements that have resulted in a restatement.

Companies that are privately owned and operated, managed as part of a private investment fund or portfolio, operated as a division within a larger company, operated under foreign disclosure requirements, or any combination thereof, may be under no obligation to provide ongoing detailed disclosures about either their operations or their financial statements.

### **Neustar Quarterly Certifications to the NAPM LLC**

At the close of each fiscal quarter, Neustar's Chief Financial Officer, in compliance with the various Assignment Agreements<sup>1</sup>, issues a certificate confirming Neustar's financial standing. The certifications, filed without fail since execution of the Assignment Agreements, attest to the fact that no event has occurred that would permit a termination of the Master Agreement under Section 23.1(a) (for default) or Section 23.1(b) (for financial inability to perform) and that Neustar's current financial resources will be sufficient to fund capital expenditures and working capital requirements for at least the next six months, including pending statements of work. Neustar's commitment to our customers and to our role as the U.S. LNPA is exhibited by the fact that only our CFO is allowed to provide such assurance.

### **Oversight by Neustar's Board of Directors**

Neustar's Board of Directors meets at least once per quarter to discuss matters pertinent to Neustar's operations and to review financial results. The Board of Directors' Audit Committee, composed of four independent directors, meets quarterly and is responsible for reviewing:

- Neustar's financial results
- Results of the reviews and audits of the external and internal auditors
- Findings and recommendations identified as a result of internal and external audits
- Risk assessment and monitoring

---

<sup>1</sup> On November 30, 1999, Lockheed Martin, Neustar, and the NAPM signed seven Assignment Agreements, one for each U.S. region, under which Lockheed Martin assigned to Neustar, and the NAPM LLC consented to such assignment, the Master Agreements, the User Agreements, and the material hardware and software used to provide NPAC services.

Unique to Neustar, our Board also includes a Neutrality Committee whose members are Neustar's CEO and two independent board members. The Committee is responsible for reviewing neutrality reports, neutrality audits, and the status of the corporate neutrality programs (such as annual training and quarterly certifications) and that they occur without exception and on time. The Committee is also responsible for investigating any potential neutrality violations and requiring necessary corrective action.

### **Neustar Does Not Propose to Use Third-party Partners or Subcontractors**

The Industry is requesting detailed financial and neutrality information for any third-party partners or subcontractors proposed. Given that there are neutrality, operational, legal, and strategic risks, as well as financial risks when using third parties, Neustar will not delegate U.S. LNPA duties to third party partners or subcontractors.

Some bidders may have no choice but to include partners or subcontractors in their bids due to a lack of technical expertise, cash-flow, available human resources, or particularly, lack of neutrality. Neustar understands the unique requirements of successful NPAC operation, which extends all the way to the building of a corporate culture around the concepts of reliability, confidentiality, and neutrality.

### **Conclusion**

With Neustar, the Industry already has the best U.S. LNPA: Neustar has unquestioned neutrality; we are US-based; we are publically traded, not privately owned; we provide the utmost in financial reporting transparency and rigor; our financials are our own and not those of a disconnected or uninterested corporate parent; we are proposing to provide the entire LNPA service without the assistance of, and the risks associated with third party providers and subcontractors; and, importantly, Neustar's record of U.S. LNPA customer service is simply outstanding.



## 2.3 Neustar's Neutrality

---

### Why Neustar

- Meets or exceeds all VQS and RFP Neutrality Criteria today
- Neutrality Code of Conduct, developed in collaboration with the FCC and Industry, is in place today
- Successful, corporate-wide Neutrality Compliance Program in place today
- More than 60 numbering-related neutrality audits passed since Neustar's creation in 1998
- Neutrality Legal Opinion provided by an independent law firm with more than a decade of experience in reviewing LNP neutrality
- Long history of neutrality can give Industry confidence of neutrality continuing into the future
- No complex or time-consuming neutrality cure required

---

VQS Section 3.4 requires that the Primary Vendor and all Subcontractors must "at all times be Neutral Third Parties" and the RFP requires each of the regional LNP databases be managed by an LNPA that is "neutral and independent from Telecommunications Carriers." Further, the RFP Section 4.2 requires an audit of an LNPA's neutrality to be conducted every six months.

Neustar has an unquestioned record of neutrality in numbering administration that simply cannot be matched by any other entity. Created in 1998 specifically to be assigned North American Numbering Plan Administrator and LNPA contracts from the non-neutral Lockheed Martin, Neustar was born into an environment that mandated neutrality from telecommunications numbering administrators. From the outset, Neustar made neutrality an integral part of its corporate essence. Neustar was a Neutral Third Party when it was created in 1998 and Neustar remains a Neutral Third Party today. Indeed, Neustar's very name is a constant affirmation of the company's continuing commitment to neutrality.

Neutrality, though, is more than just a name. Neutrality in numbering administration must be lived in practice constantly, not merely practiced when convenient. Since 1999, Neustar has been governed by a Neutrality Code of Conduct that was developed in consultation with the Commission and the Industry. This Code of Conduct was included in the Commission order approving the transfer of the NANPA contracts from Lockheed Martin to Neustar and was referenced in the agreement by which the Industry approved the assignment of the LNPA agreements to Neustar. To Neustar's knowledge, this is the only such Code of Conduct in existence today.

## NEUSTAR CODE OF CONDUCT

1. Neustar will never, directly or indirectly, show any preference or provide any special consideration to any company that is a telecommunications service provider, which term as used herein shall have the meaning set forth in the Telecommunications Act of 1996.
2. No shareholder of Neustar shall have access to user data or proprietary information of the telecommunications service providers served by Neustar (other than access of employee-shareholders of Neustar that is incident to the performance of NANPA and LNPA duties).
3. Shareholders of Neustar will ensure that no user data or proprietary information from any telecommunications service provider is disclosed to Neustar (other than the sharing of data incident to the performance of NANPA and LNPA duties).
4. Confidential information about Neustar's business services and operations will not be shared with employees of any telecommunications service provider. Neustar shareholders will guard their knowledge and information about Neustar's operations as they would their own proprietary information.
5. No person employed by, or serving in the management of any shareholder of Neustar will be directly involved in the day-to-day operations of Neustar. No employees of any company that is a telecommunications service provider will be simultaneously employed (full-time or part-time) by Neustar.
6. Warburg Pincus will not control more than 40% of Neustar's Board.
7. No member of Neustar's board will simultaneously serve on the board of a telecommunications services provider.
8. No employee of Neustar will hold any interest, financial or otherwise, in any company that would violate the neutrality requirements of the FCC or the NPAC Contractor Services Agreements (the Master Agreements).
9. Neustar will hire an independent party to conduct a neutrality review of Neustar, ensuring that Neustar and its shareholders comply with all the provisions of this Code of Conduct. The neutrality analyst will be mutually agreed upon by Neustar, the FCC, NANC and the LLCs. The neutrality review will be conducted quarterly. Neustar will pay the expenses of conducting the review. Neustar will provide the analyst with reasonable access to information and records necessary to complete the review. The results of the review will be provided to the LLCs, to the North American Numbering Council and to the FCC and shall be deemed to be confidential and proprietary information of Neustar and its shareholders.

To ensure Neustar's compliance with the Neutrality Code of Conduct, the Code requires Neustar to undergo quarterly neutrality audits by a mutually agreed third party. Thus, Ernst & Young has conducted 50 quarterly reviews of Neustar's compliance with the Code of Conduct and other neutrality rules. Each of those 50 quarterly audits confirmed Neustar's continuing neutrality and these audit reports are shared with the Commission, the NANC, and the NAPM LLC. Moreover, beginning in 2003, the law firm of Piper Rudnick, now known as DLA Piper, conducts annual neutrality audits and submits its findings to the NAPM LLC. Each of these 10 annual audits has also confirmed Neustar's compliance with the Code of Conduct. No other prospective vendor has ever been subjected to such rigorous neutrality audits.

Below, Neustar will discuss the continuing importance of neutrality in the LNPA and then explain its neutrality compliance program in greater detail.

#### *Neutrality Remains Critical to the Success of Local Number Portability*

Neutrality in telecommunications numbering administration is not an idle academic exercise. The requirement in the Telecommunications Act of 1996 that the Commission "create or designate one or more impartial entities to administer telecommunications numbering" originated out of concern that telephone numbers were such an integral component of a telecommunications service that a biased administrator could impede the development of telecommunications competition. With this directive from Congress, and sharing the Congressional concern, the Commission, in FCC 96-286 at ¶92, determined that it was in the "public interest for the number portability databases to be administered by one or more neutral third parties." The Commission continued:

Neutral third party administration of the databases containing carrier routing information will facilitate entry into the communications marketplace by making numbering resources available to new service providers on an efficient basis. It will also facilitate the ability of local service providers to transfer new customers by ensuring open and efficient access for purposes of updating customer records. . . . Neutral third party administration of the carrier routing information also ensures the equal treatment of all carriers and avoids any appearance of impropriety or anti-competitive conduct. Such administration facilitates consumers' access to the public switched network by preventing any one carrier from interfering with interconnection to the database(s) or the processing of routing and customer information. Neutral third party administration would thus ensure consistency of the data and interoperability of number portability facilities, thereby minimizing any anti-competitive impacts.

When those words were written in 1996, competition in the local telecommunications market was still a vision. Fax machines and pagers were prominent. There were clear distinctions between Service Providers who were RBOCs, CLECs, IXCs, CMRS providers, and cable operators. There were only 60 million wireless subscribers in the United States and wireless Service Providers were initially exempt from the Telecommunication Act's LNP requirements. There were no smart phones. SMS and MMS were not in widespread use. The ITU-T had only just begun the development of standards for the transmission and signaling of voice communications over Internet Protocol (VoIP) networks with the H.323 standard.

Today, in part because of LNP, the telecommunications marketplace in the U.S. has grown into the largest and most competitively robust market in the world as traditional companies, cable operators, mobile providers, and new entrants square off to compete for business and residential subscribers. Wireless is exploding; there are now 330 million wireless subscribers in the U.S. and more SMS and MMS messages are sent each month than voice calls are made. New mobile devices are appearing in the market with increasing velocity; seemingly, everyone today has a smart phone, a tablet, or both. There are hundreds of thousands of applications available for these devices and millions are downloaded each day. VoIP is commercially available and in use by consumers and corporations throughout the country.

Innovation and change are the norm for the U.S. telecommunications market now and will be in the future. New handset devices are still being launched. More tablets and other devices are being developed. Convergence in voice, text, video, and Internet is increasing. Service providers are in the middle of developing and executing LTE plans and implementations. With this innovation and change, local number portability is more important today than ever. There are more than 600 million TNs contained across the seven regional NPAC/SMS systems. More than 500 million NPAC/SMS transactions occurred in 2012 alone. The NPAC/SMS enables number conservation using Thousands-Block Pooling and is readily used by Service Providers to gain customers, retain customers, migrate customers to different networks, and to restore service to customers in the event of outages or disasters. Neustar, as the U.S. LNPA, processed billions of individual Common Management Information Protocol (CMIP) operations in 2012 in support of those 500 million NPAC/SMS transactions.

With the continuing importance of local number portability, even a relatively small failure in the administration of LNP would have a significant financial impact on carriers and damage consumer confidence in a system that is a linchpin for telecommunications competition. As the Industry knows, the NPAC/SMS is an extremely complex system the performance of which is instrumental in ensuring the success of LNP in enabling the delivery of every voice call and text message, and the provision of critical services such as telephone number management and the restoration of service in the event of a disaster. The NPAC/SMS is a critical part of the telecommunications infrastructure in the United States. Confidence in the neutrality of the LNPA is critical, not only because the LNPA is privy to competitively sensitive information, but also because all participants in the Industry must be able to trust the LNPA to operate in a manner that will not favor any particular Service Provider or Industry segment, particularly as the LNPA and Industry adapt the NPAC/SMS to accommodate the Industry's transition to all-IP networks,

A Neutral Third Party administrator is essential to ensuring consumers and businesses are able to switch Service Providers without obstruction or undue delay in the process. Positive experiences with the porting process by consumers and businesses are vital to the success of communications competition. If consumers and businesses encounter unreasonable delays in their attempts to change Service Providers or if changing providers becomes an intolerable hassle, consumers and businesses will then become less likely to attempt switching providers. Thus, communications will be compromised if an LNPA, because of corporate affiliations or contractual relationships, acts in a non-neutral fashion. A non-neutral administrator may choose not to adequately support complex mass migration transactions or may selectively enforce transaction processing rules and Industry guidelines to give favored carriers or favored segments a competitive advantage. Similarly, since the LNPA and NPAC/SMS can play a major role in disaster recovery, a favored Service Provider could offer assurances to consumers and businesses that their services will be restored more rapidly than others after a natural disaster.

The LNP administrator must also be able to represent the porting interests of the Industry at standards development committees impartially. A biased administrator can use its power to block or push for standards for the benefit of one customer or Industry segment. Indeed, such an administrator could change feature functionality of the NPAC system to benefit certain providers or Industry segments, such as by supporting certain technologies over others. This is the very essence behind the requirements that a numbering administrator not be aligned with any particular Industry segment.

The Industry must be able to trust the integrity and neutrality of its LNPA for local number portability to function as intended. The porting process necessarily requires that Service Providers share confidential customer information and proprietary business plans with the LNPA. Service providers must have confidence that their competitively sensitive information will be tightly guarded and not shared with one or more of their competitors. If Service Providers lose this confidence because of real or perceived neutrality concerns with the LNPA, the entirety of the local number portability system will cease to function efficiently. If the portability system breaks down, then non-favored Service Providers may lose business because they can no longer capture new customers, leading not only to diminished communications competition but also to reduced consumer benefit that flows from vibrant competition. Moreover, the mere perception that the LNPA is favoring an Industry member or segment, or has the incentive to do so, will result in the Commission, the NAPM, and carriers devoting increased resources to monitoring the LNPA.

Given the increasing size of the U.S. communications market, the increasing level of competition, the increasing reliance on LNP for use beyond just competitive porting, and the volume of work the U.S. LNPA has to perform, the neutrality of the U.S. LNPA is more important than ever before and will be even more important in the future.

### **Neustar's Unmatched Commitment to Neutrality**

Commitment to neutrality in numbering administration permeates all aspects of Neustar's corporate existence. Neustar's Restated Articles of Incorporation, its corporate bylaws, and even its stock certificates all contain provisions reflecting the neutrality requirements imposed on Neustar by the Commission and the Industry. Neustar views every relationship that it undertakes, acquisition that it contemplates, investment that it examines, and debt that it incurs through the prism of neutrality. Contracts are declined; acquisitions and investments refused; and neutrality provisions negotiated into Neustar's debt instruments. No other company can make these claims, just as no other company can fully appreciate the full scope of what number administration neutrality entails.

HIGHLY CONFIDENTIAL

HIGHLY CONFIDENTIAL

HIGHLY CONFIDENTIAL

Neustar periodically looks to make investments in new companies that are developing promising new technologies, in part to help Neustar develop interesting new products that it can deliver to the communications industry. Each of these potential investments is investigated to ensure the target company is not a TSP or a TSP affiliate. Moreover, even if the company satisfies that check, Neustar requires that a neutrality escape clause be negotiated in its investment agreement, so that Neustar will be bought out immediately if the target company becomes a TSP or TSP affiliate in the future. Unfortunately, a number of the companies in which Neustar has sought to make such investments have not wanted to be encumbered by the neutrality driven provision and the investments could not be made.

The neutrality rules also affect entities that invest in Neustar. Pursuant to the Commission neutrality rules that apply to the NANPA and the PA, no TSP or TSP affiliate is permitted to own more than 5% of Neustar's equity. Rather than waiting for its investors to file documentation with the Securities and Exchange Commission (SEC) indicating that their ownership went above the 5% threshold, filings that can lag significantly in time, Neustar actively monitors its investors' ownership stakes using third-party services. As soon as Neustar discovers an investor has reached a 5% ownership stake, Neustar contacts the investor to ask for certification that it is not a TSP or a TSP affiliate, that is, that the investor itself is not on the Commission's list of TSPs (Form 499 list) nor does it own 10% or more of any entity that appears on that list. If they are not able or willing to provide such a certification, Neustar asks that the investor either reduce its investment in any TSP to below a level below 10% and provide the certification, or maintain its TSP investment but reduce its investment in Neustar to below 5%. Most investors that cross the 5% Neustar investment threshold have been able to provide Neustar with certification that they are neither TSPs nor TSP affiliates. In other instances, however, investors have chosen to draw down their TSP investments and, in others, reduce their stake in Neustar.

From a major transaction such as HIGHLY CONFIDENTIAL to the occasional investment opportunities that must be reviewed, to the standard day-to-day monitoring of our investors, Neustar's commitment to neutrality is clear and unmatched.

*Neustar is the only vendor in the industry with an effective and comprehensive neutrality compliance program in place today to ensure our Neutrality through the next contract term.*

Neustar has been able to undergo the extensive scrutiny of its neutrality auditors without significant issue because it has a comprehensive neutrality compliance program in place throughout the company. Overseeing Neustar's neutrality is the Neutrality Committee of Neustar's Board of Directors. This committee, composed of Neustar's CEO and two independent board members, establishes the company's neutrality compliance program and reviews the

reports of the neutrality auditors. The committee adopted the Neustar Neutrality Compliance Procedures, which provides a plan for compliance with the Neustar Code of Conduct, the Commission's neutrality orders and regulations governing the NANPA, PA and LNPA, and the current LNPA Master Agreements. Reporting to this committee and responsible for implementing the Neutrality Compliance Procedures and handling day-to-day neutrality issues is Neustar's Neutrality Officer, currently CONFIDENTIAL.

Neustar's neutrality compliance procedures begin with neutrality training for every one of Neustar's employees and directors, no matter where located or how removed from numbering administration. Employees and directors first undergo neutrality training as part of their onboarding process into the company and then go through a mandatory neutrality training program once a year thereafter. Additionally, prospective directors are vetted for neutrality before being permitted to join Neustar's Board of Directors. Employees and directors are required to certify their neutrality when they begin employment and their continuing neutrality every quarter thereafter.

Neustar feels that it is critical all employees and directors are given this training and required to provide the certifications because neutrality issues can arise in a number of ways, and given the global nature of communications, can come up anywhere in the world. All employees must understand Neustar's neutrality obligations so that we can avoid violations and so the employees can bring potential neutrality issues to the attention of the Neutrality Officer. For example:

A Neustar employee in Europe who may want to make an investment in a European company needs to understand that Neustar must be assured that the target company is not and will not become an affiliate of a U.S. TSP. Similarly, in 2011, a Neustar finance department employee recognized a potential neutrality issue when she received a notice of a Service Provider's annual meeting. Because of her neutrality training, she immediately brought the issue to the attention of the Neutrality Officer. It was determined that Neustar had inadvertently become the holder of a small number of shares of this SP, possibly as the result of a bankruptcy settlement in favor of a company acquired by Neustar. Because the Neustar employee recognized the neutrality issue, Neustar was able to notify the Commission and its auditors of the issue, and quickly disposed of the Service Provider's shares by donating them to the American Red Cross. Corporate-wide neutrality compliance training enables the prevention of neutrality issues before they occur and the rapid identification and resolution of such issues if one does occur.



The quarterly neutrality certifications by Neustar's employees and directors, along with a quarterly neutrality certification submitted by Neustar's CEO on behalf of the company, are an important part of the neutrality audits that Neustar undergoes. These audits, which cover all of Neustar, are performed annually in accordance with Neustar's current NPAC contract and quarterly as part of Neustar's NANPA and PA contracts. As noted above, the audits review Neustar's compliance with the Neutrality Code of Conduct, developed in collaboration with the Commission and the Industry, and with the Commission's rules and orders and the LNPA Master Agreements. In the course of the audits, Neustar makes available the necessary documents for the auditors including: neutrality compliance certifications from each employee, board member, and executive officer; a management assertion letter and management compliance certification; new hire certifications; and the results of the neutrality tests given annually to every Neustar employee. The auditors also review LEAP service agreements, NPAC end user agreements, NPAC access and security, and customer transactional documentation from the NPAC, NANPA, and PA to ensure Neustar has treated each user or applicant fairly and in an unbiased manner. The auditors review certifications from each

shareholder holding a 5 percent or greater share of Neustar's outstanding stock, notices to the FCC of any organizational and board changes, as well as our debt and revenue information. Our auditors then conduct extensive internal review of the audit proceedings, findings, and reports to ensure all appropriate audit procedures were followed.

The auditors' reports are reviewed by the Neutrality Committee of Neustar's Board of Directors. The full Board of Directors also reviews the results of the audits for independence, integrity, accuracy, and irregularities, and certifies its acceptance of the audit report by attesting and forwarding it to the FCC's Wireline Competition Bureau, Enforcement Bureau, the NANC, and the NAPM LLC.

As noted above, the results of this corporate-wide focus on neutrality speak for themselves. To date, Neustar has passed all 10 annual LNPA Neutrality Audits and all 50 quarterly NANPA/PA Neutrality Audits. In the highly competitive and volatile communications Industry, this is a significant achievement. Congress anticipated the neutrality challenges facing numbering administrators when it mandated that such administrators must be impartial. Neustar faces those challenges every day. Neustar's seasoned and highly expert team minimizes those challenges and, when they arise, effectively addresses all such neutrality challenges to the satisfaction of the FCC and the Industry. Neustar will continue to place the highest importance on our neutrality compliance during the new contract term so that the NAPM and the FCC can be confident that the Industry can trust its LNP administrator not to allow its business relationship or close ties with Industry members or an Industry segment to override its obligation or cloud its judgment.

*The Neutrality Legal Opinion provided by DLA Piper confirms Neustar's compliance with the Neutrality Criteria set forth by the NAPM LLC without requiring Neustar to make any structural or procedural changes. No complex neutrality cure that may require a time-consuming approval process is needed for Neustar to continue to serve as the U.S. LNPA.*

DLA Piper LLP has furnished a Legal Opinion confirming Neustar's compliance with the Neutrality Criteria set forth in the Section 3.4 of the VQS. By mutual agreement between Neustar and the NAPM LLC, DLA Piper has for the last 10 years evaluated Neustar's compliance with neutrality requirements and so is uniquely qualified to issue a Legal Opinion regarding Neustar's neutrality. Better than any other law firm could, DLA Piper understands what to evaluate, the questions to ask, and the issues to raise in connection with an entity's compliance with the unique requirements for LNP neutrality. It is also important to note that these periodic neutrality audits represent the only business relationship that DLA Piper has with Neustar. Thus, DLA Piper truly is a neutral third party auditor, as it can evaluate Neustar's neutrality without any fear of losing other business.

The DLA Piper Legal Opinion does not require Neustar to make any structural changes to its corporate structure or make any other changes in order to be a Neutral Third Party. Because Neustar meets or exceeds the Neutrality Criteria, and because Neustar is not proposing the use of any subcontractors to provide LNPA services for the next contract term, neither Neustar nor any Neustar subcontractor must develop and adhere to any complex neutrality cure. Thus, when considering Neustar for the next LNPA contract term, the NAPM and the Commission will not have to evaluate the efficacy of a neutrality cure, a time and resource intensive effort. When Lockheed Martin announced its intent to purchase a subsidiary of COMSAT 1998, for example, it took approximately eleven months for the Commission and the Industry to resolve the neutrality issues satisfactorily.

*If a Respondent is a unit or a wholly owned subsidiary of another entity, the Respondent is not neutral if the parent company is not neutral. Likewise, a parent cannot be neutral if one of its units or subsidiaries is not.*

Some Respondents, whose parent companies or subsidiaries are either non-neutral, or likely to be found non-neutral, may attempt to restructure themselves in creative ways. Regardless of the creative structure proposed, unless a Respondent is substantially divested from its non-neutral parent company or subsidiary and is out of the non-neutral parent company's control or no longer affiliated with the non-neutral subsidiary, the Respondent will be non-neutral as well. The only true neutrality cure, if the parent company or subsidiary is non-neutral, is the substantive divestiture of the business unit or wholly owned subsidiary that intends to be the LNP Administrator from the non-neutral entity, with additional protective measures like a voting trust and code of conduct. These are similar to the neutrality cures and safeguards that were applied to the assignment of the stringent NANPA and LNPA contracts to Neustar in 1999.

Additionally, a Respondent may attempt to weaken the protections and assurances provided to the Industry by a strong neutrality regime and undermine the robust competitive marketplace by proposing unique corporate structures that will allow a large public company to more easily cloak itself in the role of Neutral Third Party administrator. However, without full, corporate-wide neutrality compliance procedures, the initial neutrality protections will be difficult to sustain. Such a Respondent may argue that only a subsidiary or portion of the company need comply with neutrality provisions or that only some contractual relationships need to be subject to neutrality review. Such arguments reveal a lack of understanding of the seriousness and complexity of neutrality compliance.

A large corporation has as much an obligation to be neutral as any other potential Respondent. In fact, the tendency of large corporations to have operational areas that do not know what other operational areas are doing, demonstrates that a corporate-wide neutrality compliance program is a necessity. Each corporate group, line of business, and operational area must be monitored continuously for neutrality compliance; otherwise a serious neutrality problem may be identified only after significant resources (time, money, marketing efforts, public commitments, etc.) have been committed to the source of the neutrality concern. When discovered, it may be too late to rectify the problem. Such a situation may result in breach of contract and a complete breakdown of the nation's LNP system. To ensure the continued stability of the nation's LNP system, neutrality compliance must be required of all components of the LNPA and neutrality compliance must be monitored at all times.

*The Industry should use broad discretion to determine whether a Respondent is subject to undue influence by parties with a vested interest in the outcome of LNP administration activities.*

As explained by the Commission in FCC Order 99-346, neutrality requirements are designed to set a clear standard to measure the LNPA's impartiality, to ensure entities seeking to participate in the communications marketplace obtain timely and efficient access to numbering resources, that no particular Industry segment, consumer group, or technology is unduly favored or disadvantaged, and that the LNPA remains neutral in order to maintain the trust and confidence of the entities that must submit sensitive data to the LNPA in its administration activities. The first two Neutrality Criteria set out in the VQS serve as objective, quantifiable measures intended to prevent the LNPA from maintaining financial or equity relationships with telecommunications Service Providers and/or affiliates that could exert control over the decisions and activities of the LNPA or otherwise compromise its impartiality. The third Neutrality Criterion requires the Industry and the Commission to exclude, if left unresolved, a Respondent that is determined to be subject to undue influence by parties with a vested interest in the outcome of numbering administration and activities, regardless of whether a Respondent satisfies the first two Neutrality Criteria. In other words, depending on the type and size of business that a Respondent has with a single TSP or a group of separate, similarly aligned TSPs (i.e., same Industry segment), the Respondent could be subject to undue influence even if the

Respondent is not a TSP or TSP affiliate and does not obtain a majority of its revenue from a TSP or issue a majority of its debt to a TSP.

For example, if a Respondent, or an affiliate of a Respondent, is providing telecommunications network operations outsourcing services to a TSP through a multi-year contract for which it receives billions of dollars and under which it accepts the transfer of thousands of TSP employees, then it would be hard to argue that such a Respondent, or an affiliate of the Respondent, is not subject to undue influence even if the first two neutrality criteria are satisfied—particularly if the Respondent or its affiliate is performing the day-to-day operations of the TSP. Likewise, if a Respondent, or an affiliate of a Respondent, derives a substantial amount of its revenue from a particular Industry segment, it would once again be hard to argue that such a Respondent is not subject to undue influence from that segment even if the first two criteria are met.

Fortunately for the Industry, the NAPM LLC, and the Commission, as attested to by the DLA Piper Neutrality Legal Opinion, neither Neustar, nor any of its affiliates, manages the network operations of any TSP. Neustar also does not derive a majority of its revenue from any particular Industry segment.

*Neutrality requirements must apply equally to prime vendors and subcontractors.*

The 2015 LNPA Vendor Qualification Survey makes clear that the Neutrality Criteria apply to subcontractors involved in providing U.S. LNPA services. This is consistent with the Commission's rule governing the use of subcontractors for NANPA and Thousands Block Pooling Administration (47 CFR 52.12(a)(2)) and with the Commission's recent LNPA procurement. The Industry must be diligent when reviewing Respondent proposals that rely on the use of subcontractors or other third parties to provide the LNPA services. Subcontractors involved in the day-to-day delivery of LNPA services must be held to the same Neutrality Criteria as the prime contractor, including the possibility of having to develop and adhere to a neutrality cure and provide relevant neutrality audits and reports. Otherwise, a non-neutral entity could use the subcontractor loophole to circumvent the NAPM and FCC's neutrality requirements. There are many areas within the provision of LNPA services where a subcontractor that is subject to undue influence is just as able as a non-neutral prime vendor to skew performance in a manner that advantages particular entities, with the same negative impact on the Industry and telecommunications competition.

Neustar does not propose to use any subcontractors in the provision of the services required by the RFP, so there are no subcontractors associated with Neustar's bid whose neutrality must be examined by the Industry or the Commission.

## **Conclusion**

The NPAC/SMS is ingrained into the U.S. telecommunications market and infrastructure more than ever before, to the point that LNP is taken for granted and expected by consumers and business seeking to change Service Providers. The NPAC/SMS is relied upon to implement the very important number conservation measure of Thousand-Block Pooling and is used by Service Providers to optimize their networks and restore service to customers in case of extended network outages. NPAC/SMS information impacts all services attached to a telephone number, including voice services and SMS and MMS messaging. LNP administration is a vital underlying service that is essential for these services to work effectively and efficiently. The unquestioned neutrality of the LNPA vendor continues to be of the utmost in importance, now more than ever.

Neustar Response to LNPA 2015 Surveys



Neustar embodies what it means to be neutral. We have been neutral since our inception over a decade ago. For Neustar, neutrality is not simply a platitude; it is the essence of Neustar as a corporation. At Neustar, our neutrality is not sheltered, fenced-off, or confined to certain groups and organizations, but is deeply ingrained throughout the entire company. Our neutrality has been inspected, audited, and verified. By retaining Neustar as the U.S. LNPA, the Industry, the NAPM LLC, the NANC, and the Commission can be assured that the neutrality of LNPA services will be maintained into and through the next contract term.

## 2.4 Neustar's LNP Expertise




---

### Why Neustar

- Meets or exceeds all LNP Neutrality Criteria
- USA's only LNP Administrator under contracts first executed in 1997
- Canada's only LNP Administrator under contracts first executed in 1998
- Processed and managed over 500 million transactions in the US NPAC/SMS in 2012 alone
- Propose providing all U.S. LNPA services without the use of subcontractors or third parties

---

The Industry in its 2015 LNPA Vendor Qualification has asked respondents to identify: 1) any U.S. LNPA service experience or U.S. LNP experience; 2) any other LNPA-like or LNP experience (presumably from other countries); and 3) any other LNP-related product experience so the Industry can assess and evaluate whether a given respondent possesses sufficient experience and technical and operational capabilities to deliver the U.S. LNPA.

Under contracts first executed in 1997, Neustar has been the only U.S. LNP Administrator since LNP was introduced. We provided the service initially as part of Lockheed Martin and then on our own as of late 1999. As the U.S. LNPA, Neustar has accomplished the following:

- Enhanced the NPAC/SMS platform including the successful management of 452 NANC change orders, over 100 Illinois change orders, and eleven major software releases
- Successfully implemented Thousands Block Pooling starting in 1998
- Successfully implemented Wireless Number Portability starting in 2003
- Successfully implemented One-Day Porting in 2011
- Processed over 12 billion CMIP Operations in 2012 alone
- Processed over 40,000 Pooled Block Requests with over 99.9% accuracy in 2012 alone
- Processed over 55,000 Mass Change Requests for over 175 companies in 2012 alone
- Refreshed the entire NPAC/SMS hardware and network multiple times

- Earned "Superior" (highest possible) rating for U.S. LNPA Customer Survey Score since 2009
- Earned highest ever Overall Satisfaction rating (3.84 out of 4.00) in the 2012 U.S. LNPA Customer Survey
- Satisfied 27 U.S. LNPA SLRs 99.94% of the time during the last five years

There is a vast difference between "being qualified to bid" versus actually being "qualified to serve." As detailed below, U.S. LNP is unique with no directly comparable LNP system worldwide except, arguably, Canada, where there are many similarities in NPAC/SMS business rules and processing. Neustar is the sole LNPA in Canada as well. If the U.S. LNPA selected for the next contract term cannot transition and operate the service competently, there will be several negative impacts, such as:

- Misrouted telephone calls and misrouted traffic for services such as SMS/MMS messages, causing increased Service Provider customer service calls and associated costs; and if long-term, customer retention problems
- Failed or slowed competitive consumer porting with reduced or slowed revenue to Service Providers and increased Service Provider customer care and resolution costs
- Failed or slowed customer retention programs and new service/mobile device launches, again, with reduced or slowed revenue to Service Providers and further increased Service Provider customer care costs
- Failed or slowed access to telephone numbers for Service Providers
- Delayed law enforcement and public safety activity, putting citizens and property at risk
- Impaired disaster recovery efforts that use porting, pooling, or network migration as a remedy
- Failed or slowed Service Provider network migrations, potentially leading to customer service outages
- Improper calls made by automated dialers to wireless telephone numbers, causing complaints to the FCC and State PUCs

Aside from having the requisite U.S. LNPA experience, Neustar also has unmatched staff expertise whereby we have hired many individuals with service provider and regulatory experience to serve in leadership positions to provide value to the Industry and the FCC. The Industry will recognize many of these people as U.S. LNP pioneers.

This approach also translates into providing superior customer service in the critical role as the nation's only LNP administrator. Over the years, Neustar has continuously improved its LNP administration service to achieve a near flawless rating in 2012. Given that a new vendor will have to focus on getting only the basic service off the ground, it is highly unlikely that any other respondent can match the level of service that the Industry has come to expect of Neustar.

*The U.S. LNPA's aggregate characteristics are not duplicated in respondents whose products or services they claim are comparable.*

Respondents will attempt to say that their International LNP experience (either from an individual country or through a combination of countries) is comparable to the United States. However, despite other international implementations of LNP since 1997, the U.S. LNP ecosystem and U.S. LNPA service continue to be unique due to:

- Large telecommunications market
- High value (life-time and monthly ARPU) of an individual telephone customer
- Number of participants connected to the centralized LNP database (NPAC) and receiving data
- Number of facilities-based service providers
- The complexity of NPAC data models
- Huge volume of transactions
- Governance structure between industry and regulatory stakeholders
- Complexity of portability business rules and short porting timeframes
- NPAC/SMS CMIP interface requirements
- Cost-recovery requirements
- Large number of Service Providers billed
- Strict neutrality requirements

International LNP deployments span the gamut of: 1) using a centralized file cabinet approach with daily batch uploads and downloads of ported telephone numbers to 2) using a distributed LNP methodology whereby no centralized LNP database exists and carriers send messages to each other when a telephone number ports to 3) being more sophisticated through the use of a centralized database system that does possess some real-time broadcast capability. International LNP deployments are generally less demanding than the U.S. For example, many International LNP deployments do not broadcast routing updates in real-time; do not allow telephone numbers to be ported between wireline and wireless providers; only identify the service provider ported to and from, and not the underlying network; and involve porting intervals of days or weeks instead of minutes and hours as in the U.S.

From an operational perspective, the various aspects of international number portability offerings typically are handled with a partnership of companies or through the use of sub-contractors. A typical International LNP deployment uses a local, in-country vendor to operate the LNP service but uses an out-of-country vendor to develop the LNP system. This approach means that much of a vendor's LNP experience in those markets is incomplete as the vendor does not perform all aspects of the administration. These types of arrangements work with varying degrees of success throughout the world, though all under far less complex and demanding circumstances than required in the U.S. The inherent problem associated with harmonizing focus and priorities, guaranteeing stability,

and applying strict neutrality rules across multiple entities, makes this approach risky and often problem-ridden. This approach becomes far riskier as the size and complexity of the system increase.

The following Exhibit 2.4-1 shows the major system functions and contract characteristics of two LNP deployments—the U.S. and India—and the substantial differences between the LNP deployments.

It is important to note that the Canadian NPAC shares a great deal of commonality with the U.S. NPAC, although the systems differ in that Canada has not implemented number pooling and annual transaction levels are significantly lower—just 4M for Canada versus over 500M for the U.S. The platforms and business rules are similar arguably making the Canadian NPAC the only comparable LNP implementation in the world. Neustar is the sole administrator of the Canadian NPAC.

LNP experience from a country like Ghana or from a collection of countries like Mexico, Chile, and Pakistan is not comparable to experience necessary to serve as the U.S. LNPA. To demonstrate just one of many differences between international LNP deployments, Exhibit 2.4-2 shows the timeframe to port a mobile numbers between various countries that have LNP. Please note that the timeframe in the U.S. is extremely low—less than 2 hours—whereby the timeframe in the rest of the world is much longer. Even if experience from international LNP deployments were comparable, respondents would likely not be using the same staff and management team for the U.S. LNPA.

Development of SOAs and/or LSMs, or an operation of an ICP service bureau is not sufficient experience to deliver the Service required by the RFP. Although these services are complementary to that of the U.S. LNPA, the experience from such is not directly comparable. There are several differences: 1) the development of these LNP-related systems and operation of LNP-related service bureaus are not subject to strict FCC-mandated neutrality requirements; 2) providers of such systems are beholden to the one or two corporate entities that provide a bulk of their revenues as opposed to being service neutral to an entire industry 3) these systems do not have to process high porting transaction volumes; and 4) these LNP-related systems and service bureaus are not subject the GEP, SLRs, and audits required of the U.S. LNPA service.

### **Neustar non-U.S. LNPA/LNP Experience**

Neustar also successfully serves as the sole LNP Administrator in Canada under contracts first executed in 1998. As shown above, the Canadian NPAC is arguably the only LNP system worldwide that is remotely comparable to the U.S. LNPA.

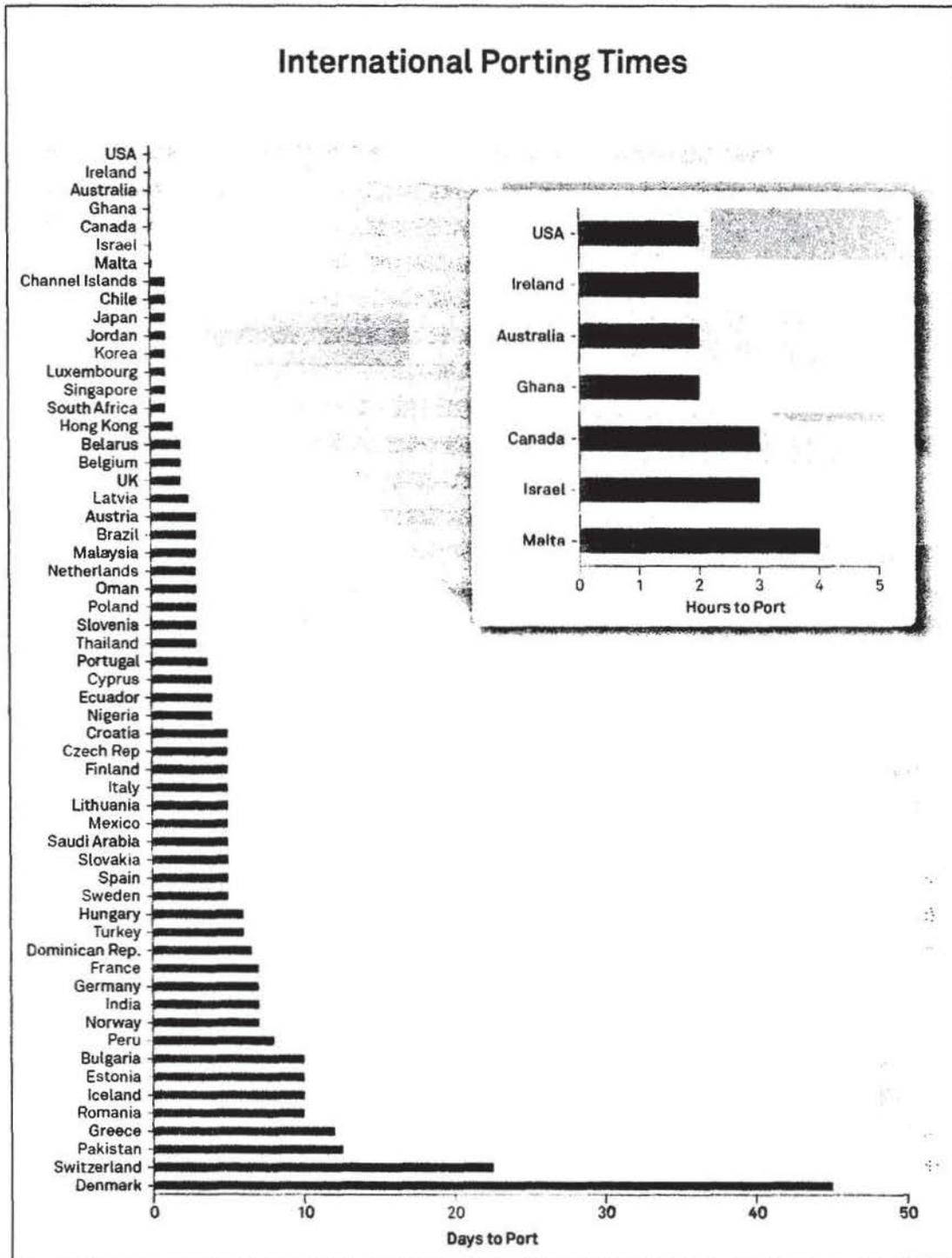
Neustar is also responsible for NPAC implementations in both Brazil and Taiwan; however, not as the LNP Administrator. In Brazil, as a subcontractor to the NPAC Administrator (ClearTech), we designed and built the NPAC system. We continue to provide software enhancements and Tier 3 support for that NPAC system. Similarly, our contract in Taiwan called for us to build the NPAC system and operate it for the first year, while training a government entity to take over operations after the first year. Neustar now provides system maintenance and Tier 3 support for the Taiwan NPAC system.

As with all foreign LNP implementations other than Canada's, these implementations do not resemble the U.S. LNP implementation at all, either in administration services, business rules, functionality, system performance requirements, or transaction volumes, and should not be considered as comparable experience.

### Comparison of LNP Deployments –U.S. Versus India

U.S. 	Contract or System Attribute	 India
<b>NPAC/LNP Administrator Governance</b>		
Yes	Single National LNP Administrator	No
Yes	Regulated Neutrality Requirements	Yes
<b>Portability/Number Pooling Implemented</b>		
Yes	Fixed TN Portability Implemented	No
Yes	Mobile TN Portability Implemented	Yes
Yes	Intra-carrier TN Porting Implemented	No
Yes	Mass TN Porting Tool Implemented	No
Yes	Porting Across Technologies (Fixed, Mobile, VOIP) Implemented	No
Yes	Number Pooling Implemented	No
<b>Porting Rules and Volumes</b>		
<b>425+ Million</b>	Annual Fixed TN Porting Volumes	<b>0</b>
<b>80+ Million</b>	Annual Mobile TN Porting Volumes	<b>40 Million</b>
<b>1,000+</b>	Number of Carriers Connected/Supported	<b>15+</b>
<b>Minutes</b>	Wireless Porting Intervals	<b>7 Days</b>
<b>ACQ/LRN</b>	Call Routing Method	<b>ACQ</b>
Yes	Recipient Carrier-Controlled Porting	Yes
<b>NPAC Features and Functionality</b>		
Yes	Detailed NPAC/LNPA Service Levels	No
Yes	Severe NPAC/LNPA Performance Penalties	No
Yes	NPAC Database Supports Enhanced Features	No
Yes	NPAC Database Identifies Reseller Relationships	No
Yes	Separate Law Enforcement Platform Implemented	No
Yes	Mechanized NPAC Data Access	Yes
Yes	Real-Time NPAC Data Distribution	No
Yes	Service Provider NPAC UI Access	Yes

**Exhibit 2.4-1:** Differences in the deployment of LNP between the U.S. and India span functionality, porting rules, and volumes. In many critical areas there is no comparison—the U.S. deployment is far more complex.



**Exhibit 2.4-2:** The time to port timeframe in the U.S. is extremely low—less than 2 hours—whereby the timeframe in the rest of the world is much longer.

**Neustar Executive Team**

Neustar's management team (shown in Table 2.4-1) provides corporate oversight of NPAC services as well as sets the strategic direction of the company.

**Table 2.4-1. Neustar's Management Team**

Name, Title	Profile
<p>Lisa Hook President and Chief Executive Officer</p>	<ul style="list-style-type: none"> <li>• President and Chief Executive Officer of Neustar, Inc. and is a director of Neustar</li> <li>• Previously served as President and Chief Operating Officer from January 2008 to October 2010</li> <li>• Held leadership positions at a number of Fortune 500 companies including AOL, Time Warner and Viacom over a distinguished career spanning more than 25 years</li> <li>• Senior advisor at the Federal Communications Commission</li> <li>• Serves on a number of other corporate and non-profit boards, including Reed Elsevier PLC, Reed Elsevier NV, Reed Elsevier Group PLC, the George Mason Honors College External Advisory Board and The Ocean Foundation.</li> </ul>
<p>Paul Lalljie Senior Vice President and Chief Financial Officer</p>	<ul style="list-style-type: none"> <li>• Oversees Neustar's worldwide finance organization, which includes treasury, accounting, financial planning and analysis, real estate management and investor relations</li> <li>• Prior to becoming CFO, served in a variety of increasingly expansive roles within Neustar's Corporate Finance department, including Vice President, Financial Planning &amp; Treasurer and other positions within accounting, financial planning and analysis, treasury and investor relations</li> <li>• Northern Virginia Technology Council's (NVTC) Public Company CFO of the Year 2012</li> </ul>
<p>Mark F. Bregman Senior Vice President and Chief Technology Officer</p>	<ul style="list-style-type: none"> <li>• Responsible for Neustar's product technology strategy and product development efforts</li> <li>• Previously served as Executive Vice President and Chief Technology Officer of Symantec since 2006</li> <li>• Prior to Symantec, served as Executive Vice President, Product Operations at Veritas Corporation</li> <li>• Prior to Veritas, served as CEO of AirMedia, a mobile content distribution company</li> <li>• Previously served in a variety of Senior Management roles at IBM – for e.g., General Manager of IBM's Pervasive Computing division, General Manager of IBM's RS/6000 business</li> <li>• Serves on the Board of the Bay Area Science &amp; Innovation Consortium and the Anita Borg Institute, which focuses on increasing the impact of women on all aspects of technology</li> </ul>
<p>Steve Edwards Senior Vice President, Carrier Services</p>	<ul style="list-style-type: none"> <li>• Oversees North America carrier sales, product management, marketing and channel partnerships for Neustar's global Numbering Services</li> <li>• Prior to joining Neustar, was chief operating officer at Regenesys Power LLC</li> <li>• Previously served as chief marketing officer for Sonus Networks Inc.; vice president of indirect sales and channel development at AT&amp;T Business Services; and president of BT Visual Images</li> </ul>

# CONFIDENTIAL

### **Neustar's U.S. LNPA Experts**

Neustar not only believes that highly relevant and directly comparable corporate experience is necessary to be successful, but that specific personnel and staff proposed for the U.S. LNPA also must be diverse, highly capable, and experienced. In this regard, Neustar's U.S. LNPA experience is unmatched. Table 2.4-2 provides concise biographies of many of Neustar's U.S. LNPA experts from the various disciplines—product management, industry relations, regulatory, customer support, software development, billing and collections, IT operations, and industry change management—that comprise the U.S. LNPA service.

# CONFIDENTIAL

**CONFIDENTIAL**

# CONFIDENTIAL

# CONFIDENTIAL

# CONFIDENTIAL

Bill Reidway,

VP, Product Management,  
Numbering Services

Over 6 years Direct LNP  
experience, 11 years telecom  
experience

- Responsible for NPAC roadmap and user experience
- Responsible for administration and customer relationships for NPAC Administrator Products (Law Enforcement Enhanced Analytical Platform & Wireless Do-Not-Call)
- Responsible for product management for ancillary Numbering Inventory and Information Services (Port PS, Resource Inventory Management System)

# CONFIDENTIAL

# CONFIDENTIAL

While not fully dedicated to the NPAC, Neustar leverages the following experts as necessary (see Table 2.4-3). These employees are either recognized thought leaders in their respective fields or have been Numbering experts, either with the Industry or with Neustar.

# CONFIDENTIAL

# CONFIDENTIAL

# CONFIDENTIAL

## 2.5 Neustar's Record of Customer Service



### Why Neustar

- Received 3.84 out of 4.00 Overall Customer Satisfaction rating for U.S. LNPA Service in 2012
- 80% resolution of calls to the NPAC Help Desk within the first contact
- Satisfied 27 monthly U.S. LNPA regional SLR measurements 99.94% of the time during the last five years
- No GEP penalties incurred in the last five years of U.S. LNPA service

Providing excellent customer service is a core function of the LNPA and requires:

- Leveraging LNP and LNPA expertise—to proactively mitigate potential issues before they become a customer problem and to resolve NPAC user issues accurately and in a timely manner.
- **Continual improvements to the service and the system**—either as a result of direct customer and audit feedback or through identification as part of our Continuous Improvement/Operational Excellence program.
- **Maintaining neutrality**—a very careful balance between customer focus and aim to please versus maintaining impartiality in attending to requests for help or activities and protecting user information. Sometimes, providing the best customer focus and service occurs when we have to tell the NPAC user “no”.

Neustar strives to provide the highest levels of customer service. As explained previously in Proposal Section 1.2.3, NPAC/SMS Monitoring, and Proposal Section 1.3, LNPA Operational Excellence, all aspects of Neustar's LNPA customer services are measured using a comprehensive set of metrics, including:

- System metrics
- 27 regional and monthly NPAC SLRs
- External benchmarking
- An annual confidential NPAC customer survey, administered by an unbiased third-party approved by the NAPM LLC.

The entire operation of the service—every component and function—is reviewed daily, monthly, quarterly, and annually and receives attention from our executive team as well. Our recent overall satisfaction score on the annual NPAC User Survey—a 3.84 out of 4.0 is our highest score ever—reflects the high standard to which we hold ourselves. As discussed below, we scored high in every individual attribute of the survey, such as Customer Service Responsiveness, Accessibility, Knowledge, and System Performance of the survey.

Neustar's record of customer service also is reflected in our other industry-wide, neutral third-party number administration services: the North American Numbering Plan Administrator (NANPA) and the National Thousands-Block Pooling Administrator (PA) where we have earned high customer satisfaction scores of "Exceeded" and "More Than Met" respectively from the NANC NANPA Oversight Working Group for 2011.

We will continue to remain customer focused in the next term.

### **Neustar's U.S. LNP Administration Customer Service Philosophy**

Neustar has achieved high customer service scores across all of our neutral, third-party numbering administration services to the telecommunications industry due to a customer-centered corporate heritage. Our company was founded to serve as the U.S. LNP Administrator and to provide other neutral third-party number administration services like NANPA and the National PA.

As detailed in Proposal Section 2.4, LNP Expertise, Neustar has made it a practice to hire individuals with service provider and regulatory experience to serve in leadership positions to provide value to the industry and the FCC. The industry will recognize many of these people as U.S. LNP pioneers.

Additionally, we do not intend to engage sub-contractors to perform any component of the U.S. LNPA duties as we believe that the use of sub-contractors creates substantial risks with respect to potential neutrality violations, security, and requires increased oversight.

Neustar has implemented employee retention programs with features designed to retain talent and experience. Towards that endeavor, we conduct quarterly employee surveys to ensure we continuously take the pulse of our most valuable asset—our employees—to inform our compensation philosophy and further enhance our employee retention programs, thereby ensuring the stability, reliability, and performance of U.S. LNP administration. Many of our employees have been with us for several years—a number of our U.S. LNPA experts identified in Proposal Section 2.4, Neustar's LNP Experience, have been with Neustar over 10 years.

Neustar has invested in tools and programs to enable employee education and training. Each position in Neustar has specific training requirements. Employees have the option to avail themselves of several training vehicles such as on-site hands-on training, online training, offsite training, and mentor training. Additionally, we send our technical operations and development staff to specific vendor training; e.g. Security-Related Information, etc. In practice, in addition to specific education, we require that our staff be fully trained and acquire all required skills prior to being allowed access to the production environment or interaction with NPAC customers. As an example, software developers must prove themselves before they can touch certain components of the NPAC/SMS software, database, system, or network. Further, every Neustar employee undergoes annual "neutrality" training regardless of their position in the company. Finally, we offer formal training on security awareness, an overview of the NPAC, LNP 101, SLRs, and the GEP.

As mentioned earlier in this section, our performance as the U.S. LNPA is reviewed daily, monthly, quarterly, and annually. This ensures quick and accurate response to any problems that might arise and allows Neustar to mobilize resources as necessary to maintain high U.S. LNPA service levels.

In general, our U.S. LNPA customer service success is a result of our focus on quality and continuous improvement.

### **User Satisfaction Survey**

As shown in Exhibit 2.5-1, Neustar has achieved improved ratings in every category of our service and has scored a minimum of 3.8 out of 4 in every attribute surveyed. This demonstrates that we take no area or component of the U.S. LNPA service lightly. The Industry has several requirements with respect to the planning, formulation, and conduct of an annual NPAC user satisfaction survey. Neustar meets all of the Industry's requirements. Further, Neustar's NPAC Customer Survey is administered by an independent auditor. We will continue to rely on an independent auditor to conduct this survey over the next term.

As part of our focus on continuous improvement, we propose changes to the survey for the next contract term. Two examples for the Industry to consider: 1) certain categories of the survey, such as New Services Rollout, would be emphasized with additional, specific questions if a greater than usual amount of category of activity was performed during the survey period; and 2) specific feedback on the NPAC Portal. As always, we will work collaboratively with and obtain approval from the NAPM LLC before making any changes to the survey or the process.



In conclusion, over the years, Neustar has continuously improved its U.S. LNP administration customer service with a near-flawless execution in 2012. The industry can be confident that superior customer service from Neustar will continue into the next contract term.

### Overall Customer Survey Scores

Categories	2008 Score	2012 Score	Trend
Customer Service	2.5	3.9	▲
Billing	3.34	3.8	▲
Industry Forums	3.38	3.8	▲
New Service Rollout	3.4	3.8	▲
Operations	3.46	3.8	▲
Overall Client Focus	3.43	3.9	▲
Overall Survey Average	3.46	3.84	▲

**Exhibit 2.5-1:** Neustar’s overall customer survey scores have consistently improved through the years thereby delivering more predictable levels of high-quality service to the Industry.