

Table 1.3-2. NPAC Industry Certifications Overview

Industry Certification	Value
ISO 9001:2000 Quality Management System	<p>Results from 2008-2012</p> <p>Security-Related Information</p> <ul style="list-style-type: none"> Validates the LNPA's performance via a neutral, third-party auditor.
TL 9000 Quality Management System Replaces ISO 9001	<p>New for the next term:</p> <ul style="list-style-type: none"> Built on ISO 9001's eight quality principles and is designed specifically for the communications industry by the communications industry. Defines unique communications quality system requirements for design, development, production, delivery, and service. Specifies measurements for companies to help evaluate effectiveness of quality implementation and improvement programs. Validates the LNPA's performance via a neutral, third-party auditor.
ISO 22301 – Business Continuity	<p>New for the next term:</p> <ul style="list-style-type: none"> 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. Validates the LNPA's performance via a neutral third party auditor.

new

new

new

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

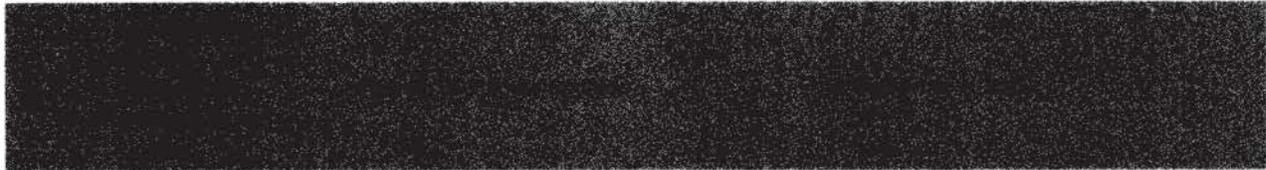
Given the complexity of the service and system delivery, there are several large organizations within Neustar focused on our success. In order to ensure these organizations are working in lockstep towards overall operational excellence, we created a function solely responsible for the overall, holistic 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
2	Scheduled Service Unavailability	As Agreed by Parties	All SLRs met in 2012
4	LSMS Broadcast Time	3 second average response time— decreased from less than 60 seconds	Average 30 millisecond response time in 2012
6	NPAC to LSMS Interface Rates	99.9% of transactions maintain a min of 7 CMIP tps— increased from 95%	Average above 99.9% in 2012 <i>New for 2015:</i> Introducing additional application layer optimization to accommodate increased throughput

New SLR	Description	RFP Requirements	Performance / Plans for 2015-2022
8	Unscheduled Backup Cutover Time	Maximum of 10 minutes to cutover to the backup site	All SLRs met in 2012
10	Full Disaster Restoral Interval	Equal to or less than 6 hrs — decreased from 48 hours	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
14	User Problem Resolution, After Hours Callbacks	99% callback within 15 minutes (outside normal business hours)— decreased from 30 minutes	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
16	Logon Administration	99.5% of all approved request within 6 hrs of receipt— changed from 12hrs and increased from 99%	100% compliance in 2012
18	System Security Remedy Invalid Access Event	Remedy logon security permission errors immediately after user notification	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		
			

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.

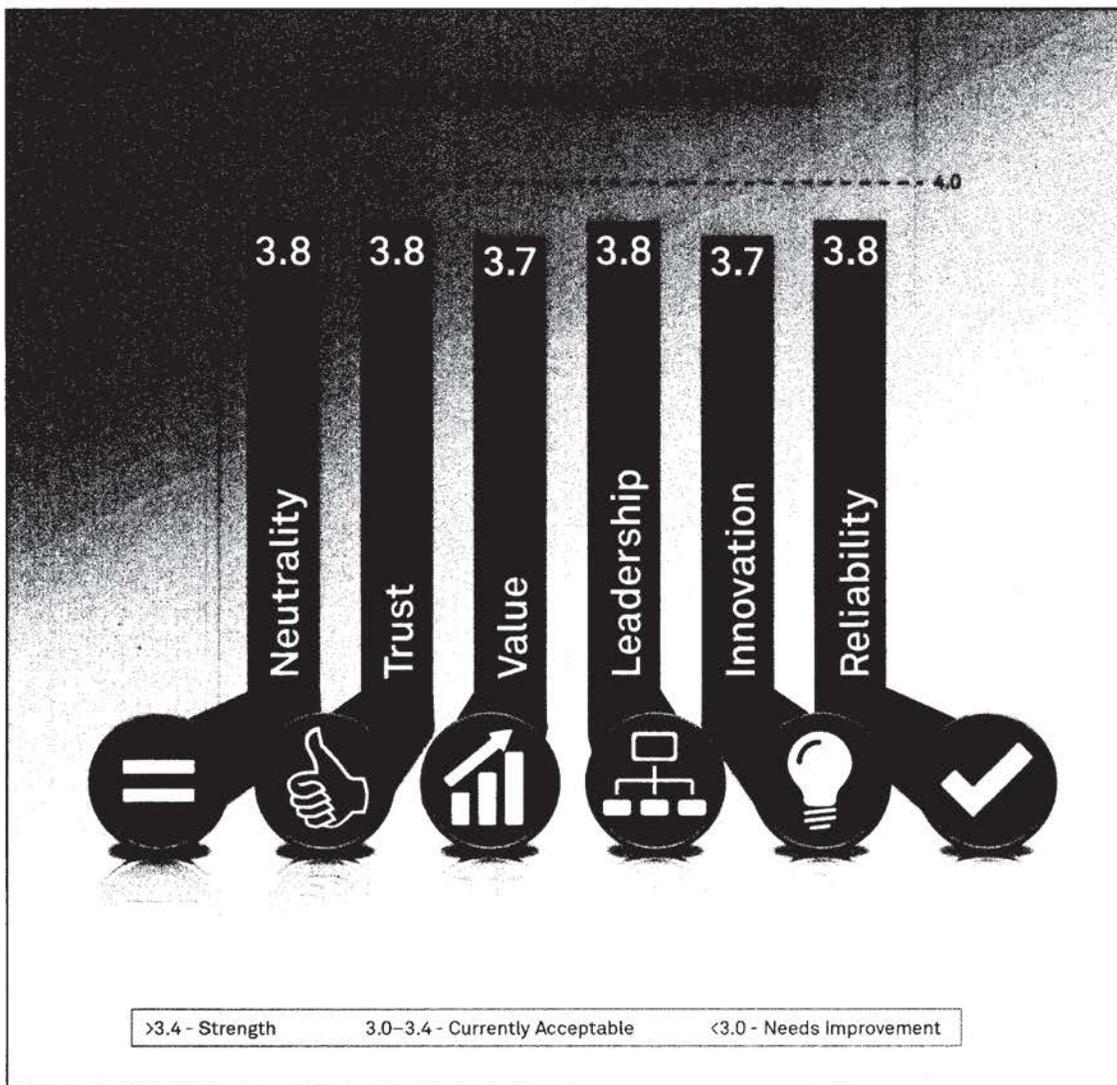


Exhibit 1.3-7: Results from Neustar’s 2012 NPAC User Survey, performed by a third-party, demonstrate our commitment to operational excellence.

064a.npac2013

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

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



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



- **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

142.npac2013

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.