

- 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' LSMSSs.

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 publically. 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 publically 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 <sup>Security-Related</sup>

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>Security-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



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:



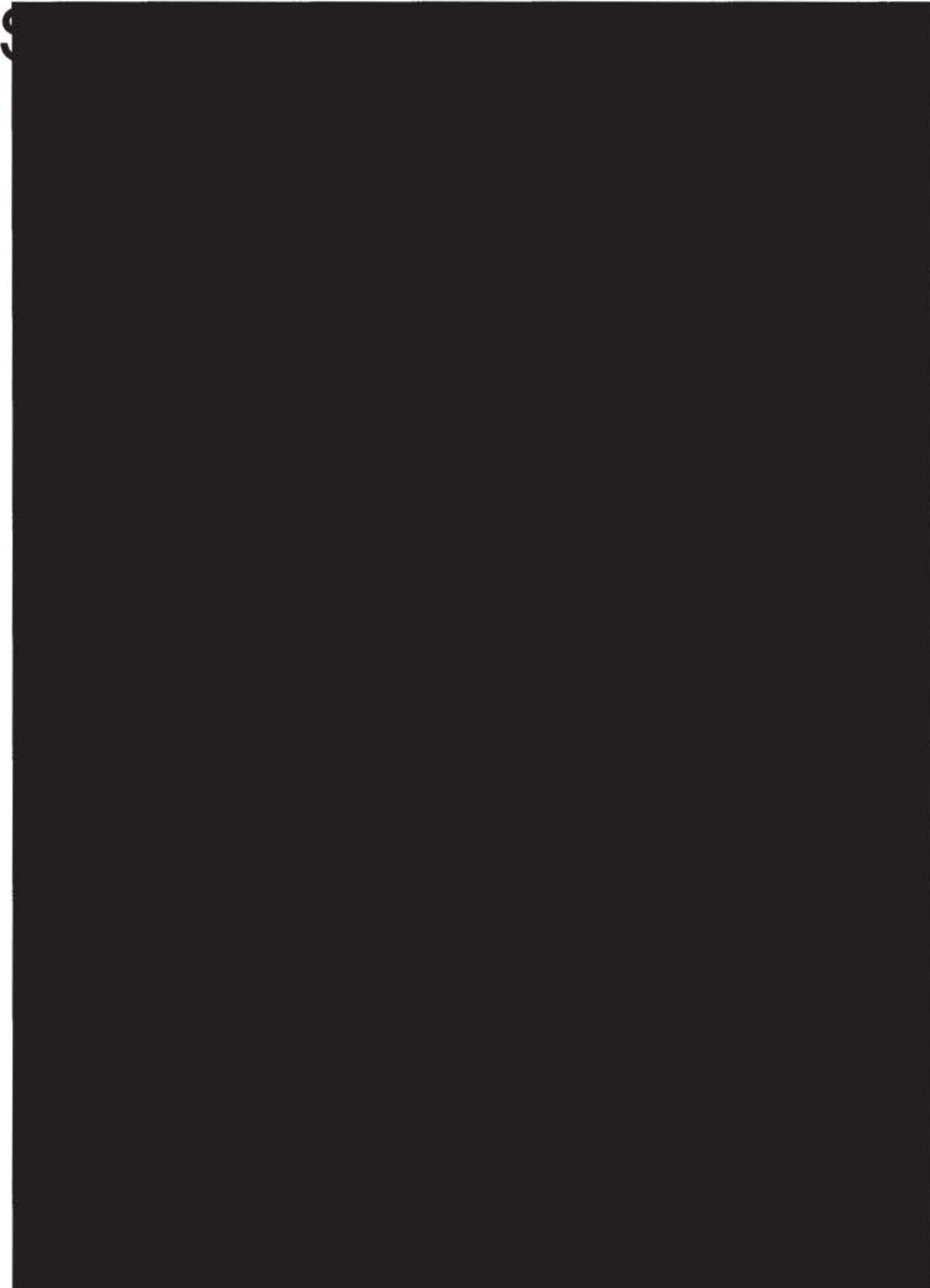
Security-Related Information

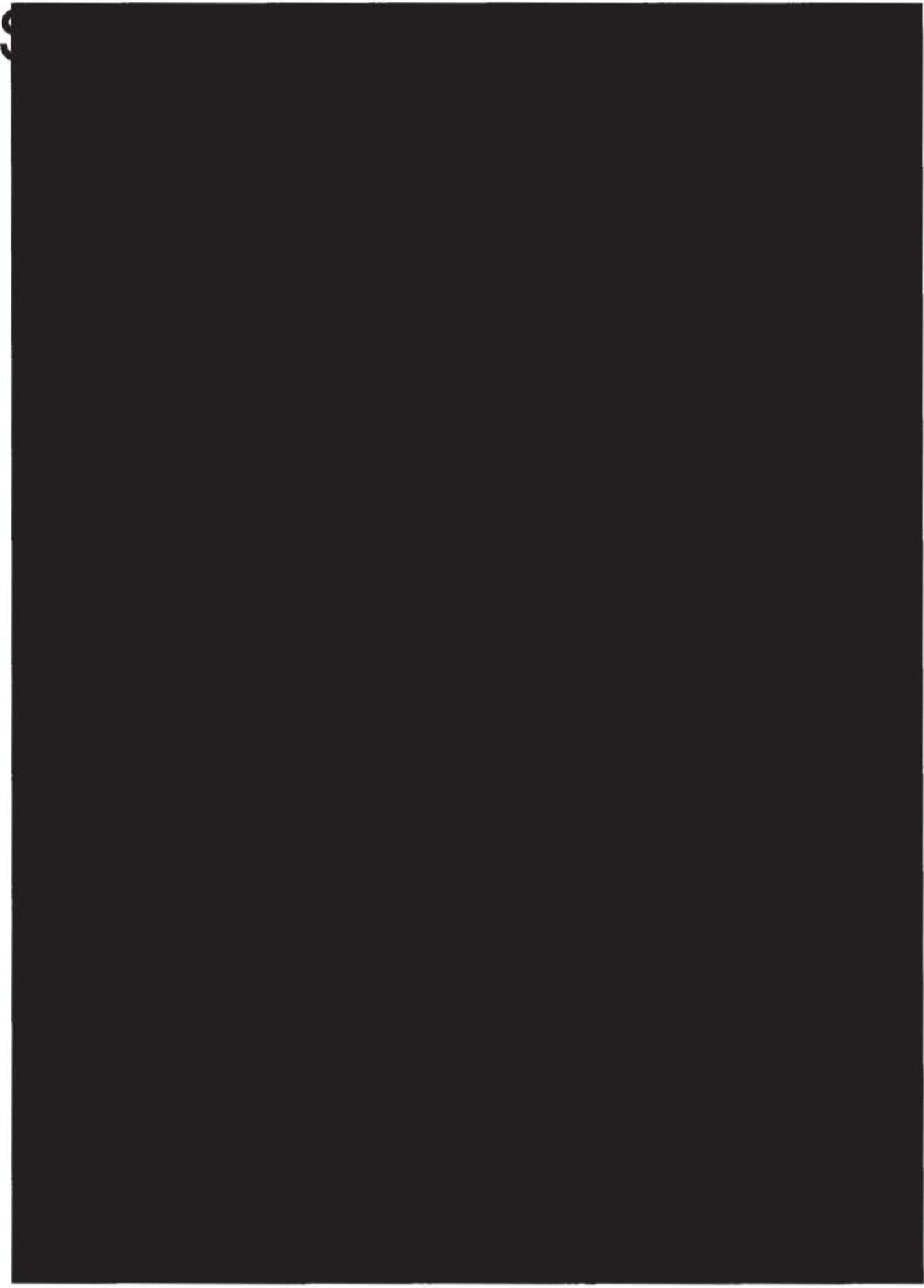
Security Related Information



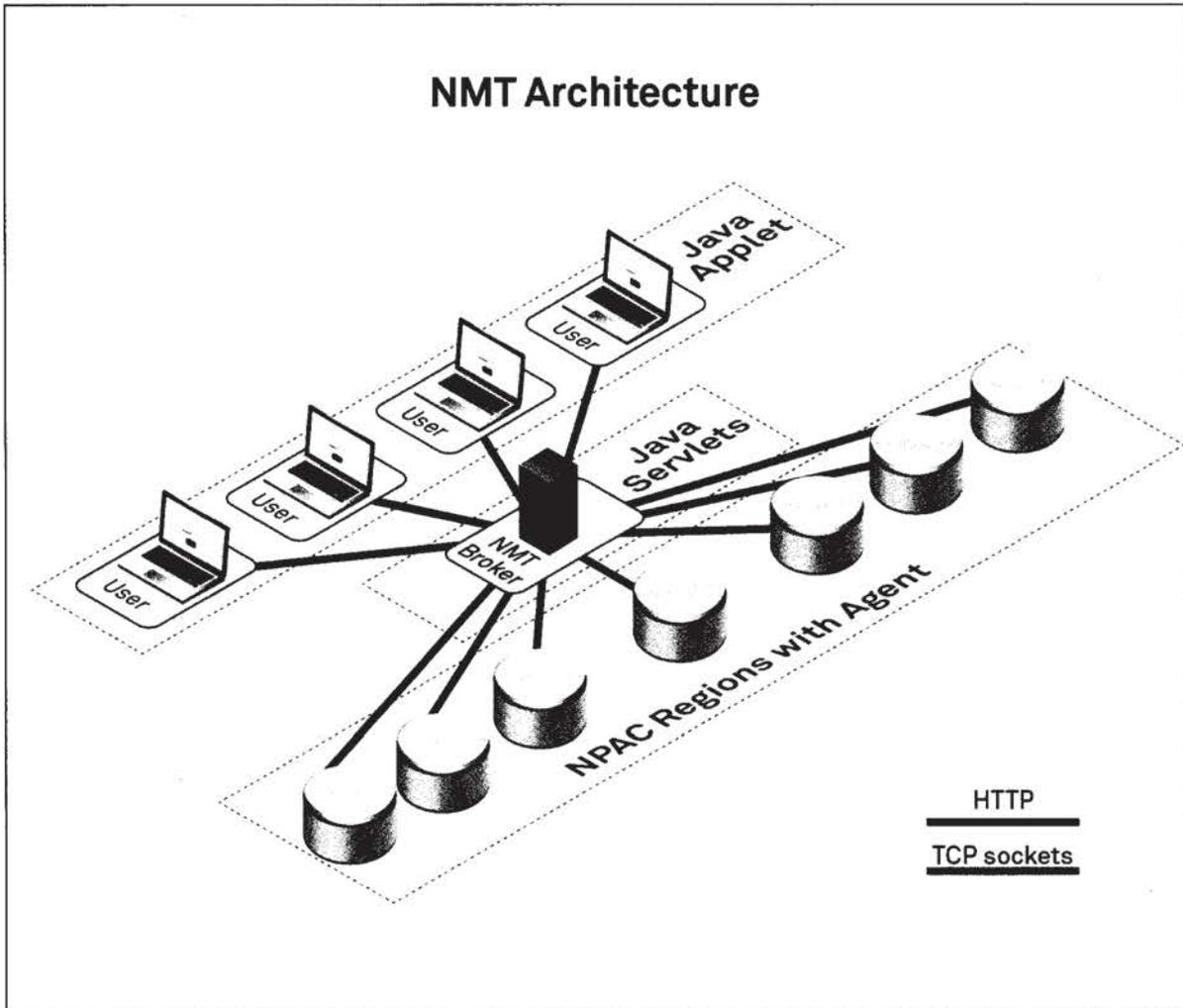
The network operations team responds to all network alerts for the NPAC. The close collaboration between NOC and network operations allows for rapid response to events and the ability to predict problems before they occur.

# Security-Related Information





# Security-Related Information



144.npac2013

**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



# Security-Related Information

