REASSIGNED NUMBERS DATABASE (RND) TECHNICAL REQUIREMENTS DOCUMENT

Description/Specifications

January 13, 2020

Reassigned Numbers Database (RND) Technical Requirements Document (TRD)

Table of Contents

Section 1: Introduction

1.1 Purpose

This document defines the Reassigned Numbers Database (RND) and the Reassigned Numbers Database Administrator (RNDA) technical, operational, and system requirements, and describes the full functionality and services required for the single, centralized database subject to the Federal Communications Commission oversight for accuracy and integrity of data.

This document serves as the reference document to other resources. The other resources include but are not limited to United States Federal Communications Commission (FCC or Commission) orders, technical standards, technical requirements and industry guidelines that support the RND and RNDA.

The technical requirements are contained in several documents. Should there be conflicts between or among these documents, the order of precedence is:

1. Code of Federal Regulations (CFR), Title 47, Volume 3, Parts 40-69, Telecommunications (Reference 11), Section 251(e)(1);
2. Applicable FCC Orders (*e.g.,* FCC 18-177)
3. Any Change Orders that have been approved by the FCC;
4. The Statement of Work in the awarded Contract;
5. Amended RND TRD document;
6. The RND TRD document;
7. Industry guidelines for the disconnected numbers being reported;
8. Related documents listed in Section 10.

1.2 Scope

This document describes the technical responsibilities of the contractor selected by the FCC to serve as the Reassigned Numbers Database Administrator (RNDA). The primary scope of this document is to define the RNDA's performance within the United States.[1] The RNDA's role and functions will include establishing and maintaining a single, comprehensive database that will enable callers to verify whether a telephone number has been permanently disconnected, and is therefore eligible for reassignment, before calling that number. The RND will contain information on disconnected US geographic and toll free telephone numbers. The RNDA will collect disconnected number data from each Service Provider that obtains North American Numbering Plan (NANP) US geographic numbers and from the Toll Free Number Administrator (TFNA) that assigns toll free numbers to Responsible Organizations (RespOrgs).[2]

The RNDA shall develop, deploy, and manage a database system that securely houses all permanently disconnected US geographic and toll free numbers and the date of the most recent permanent disconnection of each of those numbers. When a caller[3] queries the database using a NANP US geographic or toll free telephone number and a date, the database must provide a response of "yes", "no", or "no data" to explain whether the number has been permanently disconnected since the date provided by the caller.

---

[1] United States means the United States and its territories.

[2] A Responsible Organization, or "RespOrg," is an "entity chosen by a toll free subscriber to manage and administer the appropriate records in the toll free Service Management System for the toll free subscriber." See 47 CFR § 52.101(b).

[3] The term "caller" includes, but is not limited to, a person or entity that initiates any call using a wireless, wireline, or interconnected VoIP service.

The system shall accommodate the necessary volume of data and provide access to that data by multiple simultaneous system users. The system shall offer the ability to process low-volume queries (*e.g.*, via a web site interface), as well as support high-volume queries (*e.g.*, via batch process and/or standardized application programming interfaces or other protocols). The system's web interface shall facilitate mechanized data input capabilities and shall also allow for the generation of reports.

1.3 Background

The FCC's rules require telecommunications Service Providers to ensure the efficient use of telephone numbers by reassigning a telephone number to a new consumer after it is disconnected by the previous consumer.[4] Once a consumer disconnects a number, he or she might not update all parties who have had previous authorization to call. When the disconnected number is reassigned, callers may inadvertently reach the new consumer who now has been assigned the disconnected number.

Unwanted calls to reassigned numbers can be a problem for callers and consumers. Commercial databases exist to aid callers, but these databases are not comprehensive. The FCC took the first step toward addressing the problem by launching a broad inquiry in July 2017.[5] In response to the Notice of Inquiry (NOI), a majority of commenters supported establishing a comprehensive and timely database that allows callers to verify whether a number has been reassigned before making a call.[6]

In March 2018, the FCC adopted a *Second Further Notice* proposing to establish a reassigned numbers database and seeking comment on the mechanics and policies associated with the database.[7] Based on their review of the record in the *Second Further Notice,* the FCC adopted a *Second Report and Order* in December 2018[8] in which they required the establishment of a single reassigned numbers database to supplement existing commercial solutions and provide for functionality to enable callers to avoid calling reassigned numbers.[9]

Specifically, the FCC required Service Providers to report the last date of permanent disconnection associated with their allocated and ported-in numbers to a Reassigned Numbers Database Administrator (RNDA). A caller can then, if it chooses, use the database to determine whether a telephone number has been permanently disconnected after a date certain and therefore is no longer assigned to the party the caller wants to reach.

---

4 Once a number is disconnected, a Service Provider can designate it as an "aging number" for a period and subsequently reassign it to a new subscriber. *See* 47 CFR § 52.15(f)(1)(ii). ("Aging numbers are disconnected numbers that are not available for assignment to another end user or customer for a specified period of time. Numbers previously assigned to residential customers may be aged for no less than 45 days and no more than 90 days. Numbers previously assigned to business customers may be aged for no less than 45 days and no more than 365 days.").

5 *See generally Reassigned Numbers NOI.*

6 *See, e.g.,* Comcast *NOI* Comments at 10-11; NCLC *et al. NOI* Comments at 1-4; National Rural Electric Cooperative Association *NOI* Comments at 3; NCTA – The Internet & Television Association *NOI* Comments at 1 (NCTA); Retail Industry Leaders Association *NOI* Comments at 3 (RILA); TracFone Wireless, Inc. *NOI* Comments at 1 (Tracfone). A minority of commenters expressed concerns about the potential costs of a database solution versus the benefits. *See, e.g.,* American Cable Association *NOI* Comments at 4; CTIA *NOI* Comments at 14; The ETA *NOI* Comments at 2; Noble Systems Corporation *NOI* Comments at 1 (NSC); U.S. Chamber Institute for Legal Reform *NOI* Comments at 2-3.

7 *See Advanced Methods to Target and Eliminate Unlawful Robocalls*, CG Docket No.17-59, Second Further Notice of Proposed Rulemaking, FCC 18-31 (rel. Mar. 23, 2018) (*Second Further Notice*).

8 *See FCC 18-177, Second Report and Order, adopted December 12, 2018, In the Matter of Advanced Methods to Target and Eliminate Unlawful Robocalls, CG Docket No.17-59.*

9 *See Second Further Notice* at 2, para. 8.

The FCC referred operational and technical issues to the North American Numbering Council (NANC). The FCC directed the NANC to issue its recommendations, for review by the FCC, for implementing and operating the reassigned numbers database, including this Technical Requirements Document, recommended fee structure, and fee amounts.[10]

1.4 Mission and Attributes

The RNDA will function under the jurisdiction of the Federal Communications Commission as the RNDA for the United States and its territories. The RNDA operates within requirements set forth in FCC 18-177.

Offerors must demonstrate that they meet the FCC's neutrality requirements through submission of a certificate signed by a Chief Executive Officer or President that explicitly certifies the Offeror meets each requirement. The successful Offeror will be required to re-certify to its compliance at the time of award. Offerors shall be prepared to provide any other documentation verifying compliance as may be requested by the FCC.

The RNDA is the designated independent entity responsible to manage the RND in an efficient, effective, fair, unbiased, and non-discriminatory manner consistent with regulatory directives and industry guidelines, and is required to comply with FCC decisions, rules and orders, as applicable. The RNDA will adhere to all FCC requirements, orders, and policies.

1.5 Objectives

The main objectives of the RNDA include:

- Provide an independent third-party administrator service to manage the reassigned numbers database.
- Establish a single, comprehensive reassigned numbers database that will enable callers to verify whether a US geographic or toll free telephone number has been permanently disconnected, and is therefore eligible for reassignment, before calling that number.
- Focus on minimizing costs and burdens for Users, Service Providers and the TFNA, ensuring that it is reasonably affordable for all to use.
- Develop the database such that it can be updated by Service Providers, Service Provider Agents and the TNFA simultaneously with information regarding permanently disconnected US geographic and toll free telephone numbers on a monthly basis.
- Develop, implement, and maintain a portal interface for the TFNA, the FCC, database Users, Service Providers, and their agents.
- Develop, implement, and maintain a system-to-system interface including Secure FTPs and RESTful APIs for Users and their agents.
- Ensure that the data contained in the database is used appropriately and accessible to the widest possible array of system users.
- Ensure that the design of the reassigned number database supports safe harbor from TCPA liability for those callers that rely on the database to learn if a number has been reassigned.
- Facilitate the collection of start-up costs from Service Providers by assisting the Billing and Collection Agent with necessary information.
- Facilitate funding operating costs through database usage charges; and the Billing and Collection Agent to provide recovery of start-up costs to Service Providers.

[10] Fee structure, and fee amounts will be addressed in a separate document.

1.6 Responsibilities

The RNDA shall:

- Perform all day-to-day RND management, and administrative activities, as well as interact with the TFNA, Service Providers/Service Provider Agents, Users/User Agents, the FCC, and other regulatory agencies as applicable.
- Provide and maintain a system to support all day-to-day and long-term RNDA functions.

1.6.1 Management

The RNDA shall implement a planned management approach utilizing effective transactional database management skills in order to make Users/User Agents aware of the availability of the RND to meet the current and future User/User Agent needs, and to support the RNDA's overall responsibility to promote the continued viability of the RND to meet the User/User Agent current and future needs.

1.6.2 Performance

The RNDA shall be responsible for maintaining the security, reliability, performance, and flexibility of the RND. Performance instructions may be found in the *FCC Cyber Security Program* (Reference 1), including guidelines and policies referenced therein.

The updating of and access to the RND shall be user-friendly and not impose a burden on the TFNA, Users/User Agents, Service Providers/Service Provider Agents, or the FCC. The RNDA shall protect from unauthorized disclosure of sensitive information provided by Service Providers/Service Provider Agents, Users/User Agents, the TFNA, or the FCC.

1.7 Certain Obligations Bearing on Responsibility

1.7.1 Interaction with Governmental Entities

The RNDA, shall be responsible for establishing and maintaining effective and business-like relationships with appropriate governmental and regulatory bodies (*e.g.*, FCC and state regulatory agencies) and addressing policy directives from these bodies.

1.7.2 Organizational Capacity

The RNDA shall maintain the necessary administrative staffing to handle the User/User Agent access, secure online payment methodologies, technical, operational, industry, regulatory, and legal issues relevant to the management of the disconnected telephone numbers data and the date of disconnected number reports provided by Service Providers/Service Provider Agents and the TFNA. Also, the RNDA must maintain the Service Provider/Service Provider Agent and TFNA access and profiles, high volume submissions on a monthly basis and other assets to manage the disconnected telephone numbers and date of disconnect data.

1.8 Policy Objectives and Context

The RNDA shall adhere to the following broad policy objectives. The RNDA:

- Shall facilitate the ability for Users to query the RND to determine if a telephone number has been potentially reassigned.
- Shall facilitate the process of Service Providers', Service Provider Agents' and the TFNA's submission of disconnected number data.
- Shall not unduly favor or disadvantage any particular industry segment or group of system users.

1.9 Environment

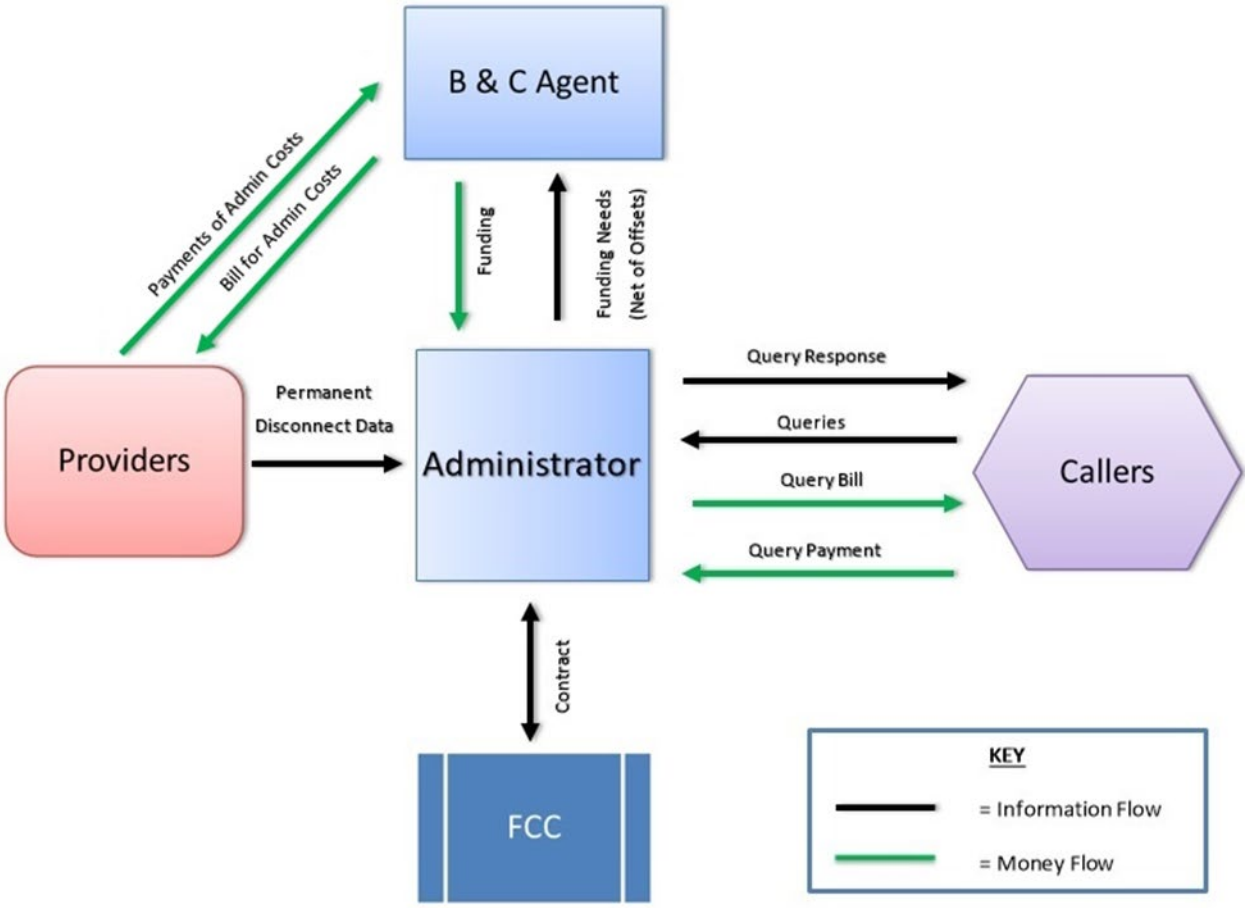
1.9.1 Regulatory

The FCC has authority over numbering within the United States. For the RND, an NOI was issued in July, 2017. An NPRM was issued in March 2018, and a Report and Order was issued in December 2018.[11] The Report and Order includes but is not limited to the following mandates:

(1) Requires the TFNA, on a monthly basis, to report the date of last permanent disconnection for each toll free telephone number allocated to US RespOrgs.
(2) Requires each Service Provider that receives NANP US geographic telephone numbers, on a monthly basis, to report the date of last permanent disconnection for each telephone number allocated to it or ported in to it.
(3) Concludes that a single database is the most efficient way to make reassigned number information available to callers.
(4) Funds start-up costs (costs to establish the database and create the query functionality) by collecting them from Service Providers using the same mechanism as other numbering administration costs.
(5) Authorizes the RNDA to fund operating costs through usage charges to callers that choose to use the database. The RNDA will be chosen through a competitive bidding process.
(6) Authorizes the RNDA to work with the Billing and Collection Agent to recoup start-up costs paid by Service Providers and to return them to Service Providers through offsets to future numbering administration charges.
(7) Directs the TFNA to revise its Service Management System tariff as appropriate to embody this responsibility of the TFNA to report the disconnect status of toll free numbers to the RNDA.[12]

The following diagram summarizes the relationships associated with reporting data, operating the database, and funding database operations:[13]

[11] *See* FCC 18-177
[12] *See* FCC 18-177, ¶23
[13] *See* FCC 18-177, ¶52



1.9.2 North American Numbering Council (NANC) Oversight

The NANC is a Federal Advisory Committee established in 1995 pursuant to the Federal Advisory Committee Act (FACA) as amended, 5 U.S.C. App 2. The purpose of the NANC is to advise the FCC and make recommendations that foster efficient and impartial NANP administration. The NANC advises the FCC on numbering policy and technical issues in areas of responsibility the FCC has entrusted to the NANC, with a focus on examining numbering in the changing, modern world of communications.

The general duties of the NANC are to gather and discuss information necessary to develop recommendations to the FCC related to numbering. Under the direction of the FCC, the NANC will provide oversight of matters relating to the RND, including the development of industry guidelines. To aid the FCC in its oversight responsibilities, the NANC will also prepare periodic and final reports for the FCC, and serve in an advisory capacity only.

1.9.3 Industry Activities

The industry develops number administration guidelines for the United States based on industry consensus and regulatory direction. The Industry Numbering Committee (INC), operating under the auspices of the Alliance for Telecommunications Industry Solutions (ATIS), is the industry forum established to develop such guidelines. The mission of the INC is to provide a forum to address and resolve industry-wide technical issues. INC guidelines incorporate federal regulatory requirements with technical and operational principles. The guidelines also recognize the existence of specific regulations in states where FCC-delegated authority has been granted.

Industry guidelines and regulatory directives are subject to change throughout the contractor's Term of Administration as the RNDA. The RNDA shall administer the RND in accordance with this TRD and any applicable industry guidelines unless they are in conflict with regulatory directives or the awarded contract, in which case the regulation or contract will apply.

Section 2: General Requirements

This document describes the functional requirements, administrative tasks, responsibilities, and duties of the RNDA. This section describes basic functions to be performed by the RNDA, described in related FCC rules, orders, or directives and the related rules, orders, including applicable industry guidelines, technical standards, and any NANC-related documentation referenced in the rules, orders or directives of the FCC, and in Section 10 in this document (which is a non-exhaustive reference list of applicable regulatory items, guidelines, and standards).

The Offeror shall describe its commitment, as well as a description of how it will adhere, to these functional requirements.

2.1 High-Level Requirements

The four (4) high-level requirements of the RNDA are indicated below.

2.1.1 Manage the RND Data and Access to the RND

The RNDA shall manage the input from Service Providers/Service Provider Agents and the TFNA to the RND, and shall manage the output to authorized Users/User Agents that query the RND. The RNDA shall ensure the RND is sufficiently robust to manage high quantities of simultaneous use and has the general functionality to meet RND Clients' needs in an efficient, effective, fair, unbiased, and non-discriminatory manner consistent with FCC regulations and industry-developed guidelines.

The RNDA shall be responsible for ensuring the appropriate safeguards are in place to protect the RND from unauthorized access, ensure the security and integrity of the data, keeping records of Service Providers'/Service Provider Agents' and the TFNA's monthly reporting, and keeping records of authorized Users'/User Agents' queries of the RND.

The RNDA shall allow for Service Providers/Service Provider Agents and the TFNA to obtain authorization level that identifies the range and scope of the data access, including identification of approved levels of access to their profile associated data.

The RNDA shall allow for User/User Agents to obtain authorization level that identifies the range and scope of the data access, including identification of approved levels of access to their profile associated data.

2.1.1.1 User Administration

The RNDA shall provide a method to grant and terminate access to the system and assign, modify, and withdraw privileges to ensure that authorized Users/User Agents have secure, transparent, and reliable access to the RND. The RNDA will authorize access to the database only to Users/User Agents who agree in writing that the Users/User Agents will use the database solely to determine whether a number has been permanently disconnected since a date provided by the caller for the purpose of making lawful calls or sending lawful texts.[14] The RNDA will obtain this certification from each new User/User Agent during

[14] See FCC 18-177, ¶26.

the enrollment process and before allowing a new User/User Agent to access the RND. The written agreement should be substantially similar to:

> *The user agrees and warrants that it, and any agent acting on its behalf, will access and use the reassigned numbers database solely to determine whether a number has been permanently disconnected since a date selected by the user, or its agent, for the purpose of making lawful calls or sending lawful texts. The date selected will be a date that the user, or its agent, reasonably and in good faith believes the person it intends to call or text could be reached at that number.*

The RNDA will accomplish this requirement by having new Users/User Agents attest, potentially as part of an online registration process, that they agree to these limitations.[15] The RNDA shall provide each approved User/User Agent with a unique system user ID and password for access to the RND (pursuant to Section 2.10.4).

2.1.2 Manage Billing for Use of the RND

The RNDA shall be responsible for billing authorized Users/User Agents for queries of the RND and collecting the appropriate payments from those Users/User Agents for such queries. In accordance with the Second Report and Order FCC 18-177 (Reference 9), and with final requirements when so determined, billing capabilities shall include both recurring and non-recurring elements, as well as query- or usage-based components.

2.1.3 Administrative Resources for Legal, Financial, and Technical Responsibilities

The RNDA shall maintain necessary administrative resources to handle the legal, financial, and technical responsibilities required to manage the RND.

2.1.4 Supervision for All Services and Responsibility for Achieving Performance Objectives

The RNDA shall provide management supervision for all of the services it provides, including responsibility for achieving performance objectives. The establishment of these objectives is a collaborative effort among the RNDA, the FCC, the NANC, and the appropriate stakeholders (e.g., INC/RND system user group).

2.2 Relationships

The RNDA **s**hall establish and maintain relationships within the United States with entities such as the FCC or others with delegated authority as appropriate. The RNDA shall cooperate with and actively participate in policy and technical numbering bodies and industry forums, such as the NANC and its subtending groups, appropriate stakeholders (e.g., INC), and any potential system user group specified by the FCC.

2.3 Administration and Management

The RNDA shall manage the RND in accordance with the most current applicable rules, orders, directives, and published industry guidelines and technical standards. Occasions may arise where decisions and interpretations are required on issues that have not yet been addressed. The RNDA shall have the knowledge and capability to recognize these instances and refer them to the appropriate body for resolution.

The contractor selected to fulfill the RNDA function shall ensure that its other contracts and business arrangements, and those of any subcontractor, do not adversely impact the RNDA organization, or resources it establishes and employs to meet these RND technical requirements.

---

[15] See also FCC 18-177 ¶26 and footnote 69

2.4 Service Provider, Service Provider Agent, TFNA, User, User Agentand Regulator Support

The RNDA shall serve as the information resource for Service Providers/Service Provider Agents, the TFNA, Users/User Agents, and the FCC (*i.e.,* Clients) concerning disconnected numbers in the RND. The RNDA shall respond to inquiries about the RND, but shall not disclose any Service Provider-specific information. The RNDA shall provide, upon request, information on how to obtain current documents related to the RND (*e.g.,* application for access to the system, user guides, secure FTP [sFTP] or RESTful API specifications) by referring to specific RNDA web pages where requesters may download electronic copies or to other sources as appropriate. The RNDA shall provide copies of documents it generates by email if the document is not available via the Internet. A list of documents related to the RND is provided in the List of References in Section 10 of this document.

The RNDA may consider offering and providing periodic online educational sessions for Service Providers/Service Provider Agents, the TFNA, Users/User Agents, and/or the FCC, and also may consider providing training videos on various topics that may be downloaded from its web site.

2.5 Cost Allocation

The Billing and Collection Agent[16] shall implement the final allocation methodology for sharing initial development costs of the RND among Service Providers in accordance with the Billing and Collection Agent Requirements Document, or appropriate regulatory documentation. Should cost allocation disputes arise, the Billing and Collection Agent shall request FCC guidance. In no circumstances shall the RNDA decide on its own the cost methodology or allocation among Service Providers.

Once the RND has been established, Service Providers shall have no further RND funding obligation as defined in the RFP. Ongoing operational costs and enhancements, including change orders, shall be recovered by the RNDA through the rates charged to the Users/User Agents.

2.6 Staffing

The RNDA shall maintain the necessary staffing levels to support industry and regulatory work relevant to the management of the RND.

The RNDA shall file an initial staffing report at the start of the contract, which shall include staffing numbers by labor category. Thereafter, the RNDA shall report to the FCC on a monthly basis that there has been no change in staffing or, in the event of a change, the report shall show shortages and overages, and yearly turnover rate.

The RNDA shall maintain necessary administrative resources to handle the legal, financial, and technical responsibilities connected with the management of the RND. Because the RNDA may occasionally interface with the media and the public as needed, the RNDA shall retain personnel that can create and maintain a publicly available web site for this purpose, and retain personnel with public relations skills (*e.g.,* the ability to explain RND administration issues to the media and the public).

To support its staff, the RNDA shall maintain the necessary equipment (*e.g.*, inventory systems, facilities, and proper billing arrangements associated with day-to-day management of the RND).

The staff shall be trained or have equivalent experience in the areas of customer service and information technology, including, but not limited to:

---

[16] 47 CFR §52.16

- Email, web-based software applications and navigation tools, and Internet browsers
- Telephone and call tracking systems and tools
- Problem and change tracking systems and tools
- Ongoing training
- Transactional database management (including data submission/update/query)

All employees and subcontractors of the RNDA who have access to a Service Provider's/Service Provider Agent's, TFNA's or a User's/User Agent's confidential information shall be U.S.-based and shall execute a non-disclosure agreement that remains in effect following the termination of employment.

Subcontractors may be used by the RNDA to perform work, but responsibility for matters contracted remains with the RNDA, which shall exercise appropriate surveillance of subcontractors to ensure effective management of its responsibilities under this contract.

2.6.1 Availability

Staff shall be available a minimum of five (5) days a week, as defined in Section 2.6 of this document. The RNDA is required to obtain prior approval from the FCC or its designee to any exception to this.

2.6.1.1 Core Hours and Daily Operations

To be available during the business hours of its continental US-based Clients, the RNDA shall be available between 8:00 am and 5:00 pm Monday through Friday local time of the continental United States, excluding recognized holidays. Since the RNDA service area covers multiple time zones, the RNDA shall provide a mechanism (*i.e.*, voicemail and/or e-mail) to be accessible on a 24-hour basis in order to meet the needs of all of its Clients. Contact information shall be readily available on the RNDA web site. The RNDA is required to give a 24-hour notice on any exception to the above via the RNDA web site.

On occasion, if circumstances warrant, the RNDA shall be available at other times to meet the needs of its Clients (*i.e.,* Service Provider/Service Provider Agents, the TFNA, Users/Users Agents and the FCC).

2.6.1.2 Holidays

The RNDA shall observe the following holidays: New Year's Day, Memorial Day, US Independence Day, Labor Day, Thanksgiving Day, Day after Thanksgiving, and Christmas Day. The RNDA shall be open for business on all other days that are neither a Saturday nor a Sunday. In all but the most exigent circumstances, emergency closures must first be discussed with the FCC's Contracting Officer's Representative (COR).

2.6.2 Inquiry Response

The RNDA shall respond within one (1) business day (to be defined in the time zone where the inquiry was originated) to general inquiries or questions, including those made outside normal business hours, whether made by email or voicemails. All emails and voicemails, whether received or responded to outside the normal business hours will be subject to a performance metric and process to be approved by the FCC or its designee. All exceptions shall be noted and brought to the attention of RNDA management.

The RNDA shall monitor and report on its response rates to Client inquiries. This report shall be furnished to the FCC upon request and used to review the RNDA's customer service activities.

The RNDA shall develop and implement an internal, documented performance monitoring mechanism and shall provide such performance review on at least an annual basis or upon request of the FCC, or its designee. The annual assessment process will not preclude Users/User Agents, the TFNA or Service Providers/Service Provider Agents from identifying performance problems to the RNDA as they occur, and from seeking expeditious resolution.

If Users/User Agents, the TFNA or Service Providers/Service Provider Agents identify performance problems, the RNDA shall investigate and report within 10 business days of notice to the Client of corrective action, if any, taken or to be taken. The RNDA shall be permitted reasonable time to take corrective action, including the necessity of obtaining the required consent of the Commission.

2.6.3 Requests for Information and Referrals

The RNDA shall, upon request, provide information and answer questions regarding the RNDA and reassigned numbers database processes, procedures, interfaces, and services within one (1) business day. The RNDA shall, upon request, provide Clients or potential Clients with assistance in understanding how to verify whether a telephone number has been permanently disconnected, disconnected number data collection, reporting and all other obligations required by the FCC.

In addition, the RNDA shall provide, within one (1) business day of receipt of a request, information on how to obtain documents related to the RND, by either referring the requestor to web sites where the information is available or by providing electronic copies of the information via e-mail to the requestor.

2.6.4 Physical Location

The physical location of the RNDA facility(s) is at the discretion of the contractor but shall be within the continental United States. The RNDA shall notify Clients and the public, by appropriate means, prior to any facility relocation or telephone number change.

2.6.5 Travel

The RNDA shall participate in RNDA applicable meetings via audio or video conference when necessary (*e.g.*, for NANC meetings or other meetings). The RNDA shall maintain staff that is available to travel in compliance with FCC requests.

2.6.6 Conflicts

Staff members of the RNDA must be fair and impartial and shall not be aligned with any particular telecommunications industry segment and may not represent the interests of the parent company contracted as the RNDA in any respect. The RNDA may not be an affiliate of any telecommunications Service Provider. The RNDA must be an independent, non-governmental entity that must meet strict competitive neutrality requirements.[17]

Conversely, neither representatives of the RNDA's parent company nor any divisions or departments thereof that are not direct, 100% dedicated employees of the RNDA may represent the interests of the RNDA.

[17] *See* FCC 18-177, ¶33

2.6.7 Subcontractors

Subcontractors may be used to perform work under the awarded contract. Subcontracting with small businesses will be in accordance with *Federal Acquisition Regulation (FAR) Section 52.219-9, Small Business Subcontracting Plan* (Reference 12).

2.6.7.1 Subcontractor Responsibilities of the RNDA

The RNDA shall provide the following information to the FCC Contracting Officer concerning each prospective subcontractor within five (5) business days of the date of official selection or within 30 calendar days of hiring any subcontractor:

- Complete name of the subcontractor
- Complete address of the subcontractor
- Type of work the subcontractor will be performing
- Percentage of the work that the subcontractor will be providing
- Evidence of the work the subcontractor will be providing
- A written statement, signed by each subcontractor, which clearly verifies that the subcontractor is committed to render the services required by the contract
- Evidence, as set out in relevant sections of the Request for Proposal (RFP), that the subcontractor meets all applicable neutrality requirements
- Written proof that the subcontractor has executed a non-disclosure agreement

2.6.7.2 Substitution of Subcontractors

The substitution of one (1) subcontractor for another may be made only with the written consent of the FCC.

2.7 Telecommunications Requirements

The RNDA shall have voice and data capabilities in order to communicate with all Clients (e.g., authorized Users/User Agents, the TFNA and Service Providers/Service Provider Agents) and the public concerning the RNDA. Each RNDA staff member who has responsibilities for interfacing with Clients shall have a direct dial number that allows direct telephone access to the staff member and the ability to leave a voice message for the staff member if he or she is unavailable. Further, the RNDA shall maintain a toll free telephone number for a Help Desk; the Help Desk shall be available to assist prospective and authorized Users/User Agents, Service Providers/Service Provider Agents, and the TFNA.

2.8 RND/RNDA Guidelines

The RNDA shall participate in the development and modification of applicable guidelines and procedures, which may or may not affect the performance of the RNDA functions. These changes may come from regulatory directives and/or industry-initiated modifications to guidelines. In addition, new guidelines may be developed as appropriate to comply with regulatory directives. The RNDA shall implement any changes determined to be consistent with regulatory directives.

The RNDA shall:

- Provide, in real time, technical guidance to ensure processes and procedures are effective in meeting the goals of the change
- Provide issues and contributions, and be prepared to discuss at INC meetings how the proposed change promotes the RND efficiencies and how the change will affect the RNDA's duties, obligations, and accountability

- Assess and share in real time (*i.e.,* during discussion) the order of magnitude cost implications and administrative impact of the change upon the RNDA's duties and responsibilities in sufficient detail as needed by the INC

Within seven (7) business days of a change, the RNDA shall provide its interpretation of the change, its impact upon service, the date the new change is proposed to become effective, what steps in current procedures need to change and when any new forms or procedures will be required. The RNDA shall provide this information to the FCC and the NANC or its designee. When the INC places any changes to its guidelines in initial closure, the RNDA shall submit an assessment (*i.e.,* a Change Order) regarding the impact of scope of work, time and costs to the INC, the NANC and the FCC within 30 days.

The RNDA shall post changes in procedures on its web site(s) prior to the change taking effect and shall notify its Clients of such posting.

The NANC or designee shall be consulted at the FCC's discretion regarding the suggested implementation date of such changes to determine the likely impact on Client processes and systems (*i.e.*, whether it would be unduly burdensome or would unfairly disadvantage any Client or group of Clients per the RNDA's obligations).

Specifically, the RNDA shall:

- Notify all interested parties when guidelines have changed and provide a short description of the changes.
- Interpret guideline changes and impact upon processes.
- Identify the implementation date or effective date of such changes.
- Provide notification of new forms or tools that may be required.
- Identify a Single Point of Contact (SPOC) within the RNDA's staff to answer questions.

2.9 Dispute Resolution

The RNDA shall resolve disputes and participate in dispute resolution as necessary. These disputes could arise from the performance of RNDA activities, from industry forum/user group activities, or from conflicting government or regulatory policy directives. The extent of involvement of the RNDA in the resolution of disputes shall depend on the nature and origin of the dispute. The Dispute Resolution process, established by the NANC, shall be followed for determination of the controversy.

The RNDA shall administer the RND based upon regulatory directives and industry guidelines. A disagreement may arise among Clients and the RNDA. The RNDA shall be required, based on the relevant regulatory directives, guidelines, and the NANC Dispute Resolution process, to address and, if possible, resolve the disagreement.

The RNDA shall interpret and apply relevant guidelines, directives, and Orders, including those listed in the *Index to the Binder of Decisional Principles* (see www.nationalnanpa.com), to resolve a disagreement when managing the RND. The RNDA shall, in all cases, follow FCC rules and the relevant guidelines that are in effect at the time that the dispute arises.

Disputes may also arise regarding reassigned numbers (Permanent Disconnection) activities. When this occurs, the RNDA may be requested to participate in dispute resolution by providing guidance and/or historical data. The RNDA shall abide by the NANC Dispute Resolution process. The RNDA shall provide any information it has relative to the dispute to the appropriate group responsible for resolving the dispute. The RNDA shall investigate the problem and report back within ten (10) business days from the

date of the complaint, to the FCC, the NANC, and to the Client on the results of such investigation and any corrective action taken or recommended to be taken.

For all disputes, concerns, complaints, and issues raised by Clients, oral or written, the RNDA shall prepare a document that contains:

- Description of the dispute, concern, complaint, or issue (recorded within one (1) business day)
- Plan of action (recorded within one (1) business day)
- The resolution and reasoning (recorded within one (1) business day of resolution)
- Number of business days passing before referred to appropriate regulators
- Number of business days passing before resolution accepted by complainant

The RNDA, in coordination with the FCC, shall take any necessary corrective action within 30 calendar days of the complaint.

The RNDA shall be responsible for expenses that are incurred in achieving compliance with any law, regulation, audit or contract requirements.

2.10 Data Security

Because of the proprietary and/or sensitive nature of some information that may be sent to the RNDA, proper security measures shall be taken. The RNDA shall be responsible for maintaining the security, reliability, performance and flexibility of the RNDA administration system. The system shall protect the sensitive information provided by Clients or any other source of proprietary, confidential, or private information.

The RNDA shall protect any Client-specific data designated as confidential, unless otherwise directed by that Client. These measures shall conform to *FCC Cyber Security Program* (Reference 1), including guidelines and policies referenced therein.

Complete information describing the security mechanisms used to prevent unauthorized access to its computers and telecommunications equipment, including internal policies, procedures, training, hardware and software, etc., will be furnished in the RNDA's Security Plan.

The RNDA is also subject to security provisions in other sections of this document.

2.10.1 Secure Work Area

All work areas shall have limited access and secured record retention practices to ensure that Client-specific data is afforded the level of security required to maintain its designated security status. The RND administration system shall have, at a minimum, security measures that are in conformance with the *FCC Cyber Security Program* (Reference 1). Systems shall include appropriate security measures for confidential data and accessibility for all Clients to their own information through an appropriately secured mechanism.

2.10.2 Physical Security

The RNDA shall provide suitable security for any and all computer systems that contain disconnected number information and/or proprietary information. This includes any system that is connected to any communications network. The RNDA shall maintain and enforce physical security procedures that conform to the requirement to maintain confidential and proprietary information. The RNDA also shall be responsible for the activities of any subcontractors to ensure the security of all systems and data, including requiring all subcontractors to execute a nondisclosure agreement. The RNDA shall ensure that

any data requested by a governmental non-RND entity is protected as confidential by that entity through applicable law or another documented nondisclosure mechanism.

2.10.3 Site Visits

The FCC, with or without notice to the RNDA, shall have the right to make visits to the RNDA facilities to review safety/security requirements. If the safety and physical security procedures do not comply with those specified, the RNDA shall correct such noncompliance within ten (10) business days. In the event of noncompliance, the RNDA shall implement corrective measures and give notice of such implementation to the FCC, and the FCC may make one or more follow-up visits to the affected site, as necessary, to confirm that the deficiency has been rectified. The FCC's rights under this paragraph shall not in any way limit the FCC's ability to visit any site for reasons other than a safety/security visit.

Inspections shall include, but not be limited to, the facilities of subcontractors, RNDA or subcontractor maintenance organizations, and remote workstations used to process RNDA data.

2.10.4 Data Accessibility

The RND administration system, and any other RNDA systems containing Reassigned Numbers data, shall have User ID and password access (i.e., Logon Credentials). Formal access shall be initiated upon receipt of completed Logon Credentials request form having the proper written approvals from the requesting Service Provider/Service Provider Agent, the TFNA, the User/User Agents or the FCC. The Client's security requirement sets the correct level of record access and system capabilities. For forms and reports requiring an applicant signature, a valid User ID and password or use of an API key (as described in Section 2.15.2) shall be considered tantamount to an applicant signature.

2.10.5 Unauthorized Access

In the event that the RNDA becomes aware of an unauthorized access to its systems or Client data, the RNDA shall immediately: (1) notify the FCC and the applicable Clients by e-mail, (2) investigate the unauthorized access, and (3) subject to reasonable access, security and confidentiality requirements, provide the FCC, Clients, and their designees with reasonable access to all resources and information in the RNDA's possession as may be necessary to investigate the unauthorized access. The FCC shall have the right to conduct and control any investigation relating to unauthorized access that it determines is appropriate.

2.11 Implementation Plan

The contractor shall provide an Implementation Plan to the FCC within 30 days of contract award, and an update of the Implementation Plan 30 days prior to the takeover of RND Administration. The objective of this Implementation Plan shall be to achieve a seamless continuance of all RNDA services across Terms of Administration.

2.12 RNDA Transition to Successor

There shall be a transition from the current administrator to the new administrator should the RNDA responsibility be awarded to a new party. The contractor shall transfer, in the case of termination or at the expiration of the Term of Administration, to the FCC or designee all hardware, software, web sites and rights to software contracts and other intellectual property as outlined in the Transition Plan.

This RNDA transition is additionally subject to the termination and continuity provisions in the solicitation. All bidders shall identify transition-related costs separately, including costs for transition from its predecessor and costs for transition to a successor.

Any other equipment or contracts associated with RNDA day-to-day operations shall transfer. This shall include but is not limited to:

- RND and all its accounts and supporting documentation
- Approved cloud hosting services and cloud-based applications
- Computers and related equipment and software
- Other peripheral devices
- All RNDA records, both current and stored
- RNDA web site URL
- Also see the Transition Plan

2.12.1 Transfer Efficiency

The transfer of all property shall be performed in a manner that ensures an efficient and orderly transition of the RND System and associated equipment to a successor's environment in a fully operational state.

2.12.2 Technical Support

The contractor shall provide at least 15 business days, but up to 30 business days over a three (3)-month period, if required, of technical support to ensure a smooth transition of the system.

2.12.3 Documentation

The contractor shall provide the FCC with copies of all documentation specified in the System Documentation Plan.

2.12.4 Transition Plan

The contractor shall provide a detailed plan for an efficient and orderly transition, 180 calendar days prior to contract termination. This transition plan shall follow the format, as applicable, of the *Software Transition Plan (STrP)* (Reference 4).

2.13 Term of Administration

The contractor shall serve for a period determined by the FCC.

2.14 Supplemental Discovery

The RNDA shall undertake a study of the business processes and functions of the stakeholders, through for example, solicitation of input from those who will use the system. The RNDA shall use this study to analyze and further refine the requirements of this requirements document. Upon completion, the RNDA shall submit a detailed requirements analysis report to the FCC or its designee. This will be considered complete upon approval of the report by the FCC or its designee.

2.15 Interaction and Interfaces

The RNDA shall interact with Service Providers and Service Provider Agents, the Toll Free Number Administrator (TFNA), and Users and User Agents. The RNDA also shall interact with the media as needed.

The RNDA shall provide the following constituency interfaces:

Constituent	Interface
Service Providers	Web, email, secure FTP
Service Provider Agents	Web, email, secure FTP
Toll Free Number Administrator	Web, email, secure FTP
Users	Web, email, secure FTP, RESTful API
User Agents	Web, email, secure FTP, RESTful API
Media	Web, email

More detailed discussion of the duties and interactions with these constituents can be found in the following sections and the applicable industry guidelines.

2.15.1 Interface with the Service Providers, Service Provider Agents, and the TFNA

The RNDA shall maintain a Service Provider, Service Provider Agent, and TFNA interface to be used to receive Service Providers'/the TFNA's monthly disconnected numbers reports in standardized data and file format(s) and to provide confirmation of receipt, in a relay between the RNDA and the Service Provider, Service Provider Agent, or TFNA. Any or all of the following interfaces may be necessary, depending on the particular Service Provider, Service Provider Agent, or TFNA with which interaction is taking place, and thus, shall be made available by the RNDA: system-to-system (secure FTP) and web site (manual input and file upload/download). For example, these interfaces shall be used to receive a Service Provider's/Service Provider Agent's/the TFNA's standardized monthly disconnected numbers report and to return a confirmation receipt to the Service Provider/Service Provider Agent/TFNA after a report has been accepted by the RND system for processing. The interfaces also shall be used, where feasible, to communicate information to Service Providers, Service Provider Agents, and TFNA (*e.g.,* email notices about system maintenance, system outages, reminders for report filings, etc.), and provide Service Providers, Service Provider Agents, and TFNA with the ability to query their own records as needed, and to manage their RND system user profiles as needed. The RNDA is responsible for ensuring the availability of these interfaces. All reporting and confirmation activities facilitated in the RND system shall also be supported via a system-to-system interface including an authentication and authorization mechanism.

2.15.2 Interface with Users or Users Agents

The RNDA shall maintain a User and User Agent interface to be used by Users or User Agents (*i.e.,* callers) that wish to query the RND and to provide the results of the query, in a relay between the RNDA and the User or User Agent. Any or all of the following interfaces may be necessary, and thus, shall be made available by the RNDA: system-to-system (secure FTP and RESTful API) and web site (query/response and file upload/download). These interfaces (system-to-system and web site) shall be used to receive a User or User Agent standardized data and file format query of the RND and to return the results of a query in a standardized data and file format. For example, the web site interface may provide an interactive query and response for a single 10-digit phone number (or short list of 10-digit phone numbers). The email interface shall be used to communicate information to the Users and User Agents (*e.g.,* email notices about system maintenance, reminders for billing, notification that query results files are available for retrieval, etc.). The RNDA is responsible for ensuring the availability of these interfaces. All RND Query Request and RND Query Response activities facilitated in the RND system shall also be supported via a system-to-system interface including an authentication and authorization mechanism. Authentication and authorization for the API shall be done using an API key, which can be created and revoked by users via a web interface (API key management). Furthermore, this API shall support

uploading documents and referencing previously uploaded documents in subsequent programmatic requests.

2.15.3 Interface with the Media

The RNDA shall be required to communicate with the media to the extent permitted by the FCC, as well as federal regulatory bodies concerned with RND matters. In situations where its contractor status is not obvious to third parties, while making representations to the public, Clients, and others, the RNDA shall identify itself in such a way as to avoid creating an impression in the minds of members of the public that it is a government official. The RNDA also shall ensure that all RNDA documents or reports produced are suitably marked as RNDA products or that RNDA participation is appropriately disclosed. Information and data shared with the news media shall be factual in nature, publicly available and previously made known to the industry and regulators prior to media disclosure.

2.16 Technical Requirements Document Maintenance

The RNDA shall be required to review and update this Technical Requirements Document semi-annually and upon the implementation of any change order, and provide the updated document to the FCC or its designee. Updates shall include, but not be limited to, any new functionality added to the RND, web site, any change orders that have been implemented since the last review and update, changes to any specific industry guidelines that are referenced in the document and any industry guidelines changes that affect or conflict with language in the document.

Section 3: System Requirements

This section describes key capabilities, which are required minimum capabilities, of the RND system. The RND system shall provide all functionality necessary to accept input in standardized formats from Service Providers/Service Provider Agents and the TFNA to populate the database and to provide Users and User Agents the ability to query the database. The RNDA shall maintain the RND system to ensure that the system and the database is capable of supporting the requirements and functionality acknowledged within this document. In addition, the RND system shall have sufficient capacity to support initial and future input and User/User Agent queries as the quantity of RND entries grows significantly over time.

This RND system shall include appropriate security measures for maintaining confidential data. It shall provide accessibility for all Service Providers/Service Provider Agents and the TFNA to perform administrative checks of the data through an appropriately secured mechanism. Similarly, the RND system shall provide accessibility for all system Clients to manage their own user profile information through an appropriately secured mechanism. These security measures shall be described in the RNDA's Security Plan.

Service Provider/Service Provider Agent and TFNA data submitted to the RNDA shall be treated as confidential. Any data published by the RNDA shall be aggregated for presentation.

3.1 System Characteristics

The RND system shall utilize standard electronic commerce type functionality that allows efficient user interaction and data file transfer. Data file transfer shall be simple and easy to understand.

3.1.1 System Availability

The RND system shall possess high reliability and allow for economical and efficient system expansion as needed. The RND system shall be seamlessly available for input, processing, downloads, and user

queries. It shall be available 24 hours a day, 7 days a week, except during scheduled maintenance windows. At a minimum, the RND system shall adhere to the following availability and reliability requirements:

- Available 24 hours, seven (7) days a week.
- Availability shall meet a minimum requirement of 99.9% of scheduled up-time.
- Unscheduled maintenance downtime per calendar year interval shall be less than nine (9) hours.
- The mean time to repair (MTTR) for all unscheduled downtime per any 12-month interval shall be less than one (1) hour during core business hours and four (4) hours for non-core business hours.
- Scheduled maintenance downtime per 12-month interval shall be less than 24 hours.
- An additional scheduled downtime shall be implemented during which time the system shall only be available to accept monthly input from Service Providers/Service Provider Agents and the TFNA, but shall not be available for Client queries.

Scheduled maintenance shall occur outside of normal business hours and Clients shall be notified by e-mail and/or other electronic notice (*e.g.,* mass notification) no less than 30 days in advance of any scheduled event. Such notifications shall also be posted to the RNDA web site, and shall provide sufficient detail such Clients can determine how such maintenance may impact them (*e.g.,* changes that may affect secure FTP or RESTful API submissions).

The RND system design shall, at a minimum:

- Use an FCC-approved web service provider.
- Support system fault tolerance that shall be transparent to RND system users.
- Support a system architecture that enables continuous operation in the event of system failure including loss of AC power up to eight (8) hours.
- Support a system architecture that has the ability to identify when the quantity of simultaneous queries exceeds a specified threshold and can temporarily limit the queries so that no user's experience is negatively impacted.

If the RND system becomes unavailable for normal operations due to any reason, including both scheduled and nonscheduled maintenance, Clients shall be notified of the RND system unavailability within five (5) minutes of the outage. The notification shall be made by electronic broadcast message (*e.g.,* mass notification) and web site to Clients. When the RND system is restored to normal operations, Clients shall be notified of the RND system's availability via electronic broadcast message (*e.g.,* mass notification) and web site within five (5) minutes of RND system restoration. Notices shall be auditable.

3.1.2 RND System Query Capability

For the purpose of this document, a query is defined as the ability to request and retrieve data stored in the system. The system shall support the following query capabilities:

For Service Providers/Service Provider Agents and the TFNA:

- Need ability retrieve their data through a query capability that includes searching on following data elements stored in the RND database record and shall include TN(s), TN Range, NPA(s), NPA NXX(s), Company Identifier(s), Disconnect Date(s), Disconnect Date Range, Modify Date(s), Modify Date Range, User ID(s)

For Users/User Agents:

- Need ability to retrieve data through a query capability that provides a "yes," "no," or "no data" response based upon submission of TN(s) and Date(s).[18]
    - A "no" is provided if the date provided by the User/User Agent is subsequent to the permanent disconnect date that is contained in the RND (*i.e.,* the number has **not** been permanently disconnected).
    - A "yes" is provided if the date provided is prior to the permanent disconnect date contained in the RND (*i.e.,* the number has been permanently disconnected).
    - A "no data" is provided if the number nor a permanent disconnect date is contained in the RND.
- Retain both current and previous views of RND database record (Update transaction history) views of RND record accessible from GUI interface and thru report generation (See section 10 retention of data).

3.1.2.1 Web GUI "Quick" Search

The system shall provide Users/User Agents with a "quick" Web GUI search option (e.g., individual Telephone Number, Date of Prior Express Consent) which will be executed as described and pursuant to section 3.2.

3.1.3 System Scalability

The RND shall continue to be expandable and flexible so that it can easily expand its capacity and number of Service Provider/Service Provider Agent system users, TFNA system users, and User/User Agent system users such as, but not limited to, through:

- RND Service Provider/Service Provider Agent, TFNA record storage, both production and historic views
- RND data extract capability to provide Service Providers/Service Provider Agents and the TFNA with Audit Files for RND records stored by Service Providers/Service Provider Agents and the TFNA
- Accommodate simultaneous monthly report submissions from all Service Providers/Service Provider Agents and the TFNA that are due on the 15th of each month
- Accommodate Service Provider/Service Provider Agent and TFNA Emergency Updates submitted through the Help Desk
- Accommodate both simultaneous User/User Agent RND Query Request(s) and RND Query Response(s) processing from User/User Agent Queries at peak demand.
- Create RND Query Request Transaction Logs for Users/User Agents that are available for verification (*e.g.,* billing)

3.1.4 RND Characteristics

The RND shall have the following characteristics:

- Use of Infrastructure As A Service (IAAS), which enables RND to create code to automate routine maintenance tasks, quickly rebuild virtual servers in the event of a failure, and automatically deploy new builds
- A high level of scalability, lowering the need for infrastructure that accommodates peak usage at all times
- Component isolation, so that an issue with one component will not affect others

[18] When a caller queries the database using a NANP US geographic or toll free telephone number and a date, the database must provide a response of "yes", "no", or "no data" to explain whether the number has been reassigned (or more accurately, permanently disconnected) since the date provided. *See* also 47 CFR §64.1200 (m) (1).

- Automation functionality capability
- Allow secure and efficient Service Provider/Service Provider Agent, TFNA, User/User Agent and FCC interaction with GUI and bulk file transfer
- Allow new disconnected number record additions by Service Providers/Service Provider Agents or the TFNA to the RND database with complete individual TN record replacement and shall contain TN, Disconnect Date, and Company Identifier.
- Maintain both a current and historic record of each RND TN and the updates associated with each TN for audit purposes
- Maintain audit records for each User/User Agent
- Maintain audit records for each Service Provider/Service Provider Agent and the TFNA

3.1.5 RND Functionality

3.1.5.1 RND Fuctionality for Service Provider/Service Provider Agent and the TFNA

The RNDA shall assure that authorized Service Providers/Service Provider Agents and the TFNA are provided with the following functionality in the RND:

- Shall be provided read/write access to its Service Providers/Service Provider Agents and the TFNA account profile information
- The RND will auto populate the Service Provider/Service Provider Agent or TFNA User ID, Company Identifier, and Modify Date.
- Shall be able to upload its permanently disconnected TN data in a manner (*i.e.,* secure FTP, web interface or file upload) that allows its compliance to the requirement to upload permanently disconnected TN data on the 15th[19] of each month
- Shall be able to change or update records subsequent to the 15th of the month via the RNDA Help Desk and track such activity.
- Shall be able to submit updated files on the 15th of the month that will replace the most recently submitted file for that day.[20]
- Shall be provided confirmation of successful or unsuccessful data transmission of report and/or update files, and successful database update.
- Shall be provided with a response for database entries that are unsuccessful, identifying the error and error type (e.g., TNs with less or more than 10 digit/disconnect date in the future).
- Shall be provided capability to search/query and retrieve on a read only basis its RND database records, by TN, TN List, TN Range with search criteria that may include disconnect date, Company Identifier, Date of Updates, User ID, etc.
- Shall restrict the capability to view/query (including reports) only disconnected TN data provided by the Service Provider/Service Provider Agent or TFNA, for the purpose of demonstrating compliance and/or complaint resolution
- Shall make reports available online and in format that may be downloaded for report creation and analysis
- Shall be able to obtain assistance from the Help Desk, track and resolve issues through RND associated with the functions in this section.

---

[19] In the event that the 15th falls on a weekend or an RNDA-recognized holiday, Service Providers/Service Provider Agents and TFNA shall complete the Service Provider and TFNA Disconnected Numbers Report and submit it on the following business day.

[20] For example, on the 15th of the month a Service Provider submits a file with 200 numbers, then realizes that another 100 numbers were missing from it. The Service Provider will be able to submit a replacement file containing all 300 numbers by 11:59 pm that same day.

- Shall have Service Provider/Service Provider Agent and TFNA submissions updated into the RND within an established maintenance window immediately following the 15th of the month deadline pursuant to the Service Provider Disconnected Numbers Report and the TFNA Disconnected Numbers Report submission requirement.
- Shall provide notice to the Service Providers/Service Provider Agents and TFNA of maintenance window start and end times
- Shall be provided access to supporting documentation download – Service Providers/Service Provider Agents and the TFNA shall have the ability to download RND supporting documentation.

3.1.5.2 RND Functionality for User/User Agent

The RNDA shall assure that authorized Users/User Agents are provided with the following functionality in the RND:

- Shall be permitted to confirm its RND Query Request prior to purchase
- Shall provide an RND Query Request that includes: Telephone Number, Date of Prior Express Consent
- Shall obtain an RND Query Response that includes a response as described in Section 3.1.2 in a usable downloadable format based upon the method that the User/User Agent submitted such query
- Shall be able to provide RND data availability status via the dashboard
- Shall be provided access to a downloadable historical transaction report created for each RND Query Request that contains: RND Query Request date, number of TNs queried, number of "yes", "no", and "no data" RND Query Responses. This transaction report can be used for billing and be used to create transaction summary and summary reports.
- Shall make reports available online and in format that may be downloaded for report creation and analysis
- Shall be provided read/write access to its User/User Agent account profile information
- Shall auto populate the User/User Agent User ID and RND Query Request date
- Shall be noticed upon and an indication when the RND data has last been updated via the dashboard
- Shall be provided confirmation of a successful or unsuccessful query
- Shall be provided with a response for database queries that are unsuccessful, identifying the error and error type (e.g., TNs with less or more than 10 digit/Date of Prior Express Consent is in the future).
- Shall be able to obtain assistance from the Help Desk, track and resolve issues through RND associated with the functions in this section.
- Shall provide notice to the Users/User Agents of anticipated maintenance window and start time and real time availability via User/User Agent web access
- Shall provide access to Supporting Documentation Download – Users/User Agents shall have the ability to download RND supporting documentation.

3.1.5.3 RND Functionality for the FCC

The RNDA shall assure that authorized FCC users are provided with the following functionality in the RND:

- Shall be provided read/write access to its FCC User account profile
- Shall be provided the capability to update its FCC User ID profile as needed

- Shall be provided capability to search/query and retrieve on a read only basis any and all RND database records, by TN, TN List, TN Range with search criteria that may include disconnect date, Company Identifier, Date of Updates, User ID, etc.
- Shall make reports available online and in format that may be downloaded for report creation and analysis
- Shall be able to obtain assistance from the Help Desk, track and resolve issues through the RND associated with the functions in this section.
- Shall notice the FCC with the Service Provider/Service Provider Agent and TFNA maintenance window time period.
- Shall provide access to supporting documentation download – The FCC shall have the ability to download RND supporting documentation.
- Shall be permitted to query the RND for compliance or verification purposes in the same manner as a User/User Agent but at no charge
- Shall be provided access to a downloadable historical transaction report created for each of its RND Query Requests that contains: RND Query Request date, number of TNs queried, number of "yes", "no", and "no data" RND Query Responses.[21]
- Shall be noticed upon and an indication when the RND data has last been updated.

3.2 System Capabilities

The RND shall be designed for high reliability, possess data integrity features, and allow for economical and efficient system expansion. The RND shall:

- Capture all relevant Client information
- Pre-populate relevant Client queries and data updates from the Client system user profile where possible (*e.g.,* contact information, Company Identifier name)
- When the Company Identifier is required on an RND data update, allow the Service Provider Agent to select the appropriate Company Identifier in the Service Provider/Service Provider Agent's profile via a drop-down menu
- Facilitate the Service Provider/Service Provider Agent and TFNA report submission process and the capture of required data in the database
- Support ad hoc Service Provider/Service Provider Agent and TFNA query capability as well as production of predefined reports
- Possess the ability to provide historical TN and disconnect date data via GUI access and via reports for approved designated entities
- Possess the ability to track the status of a User/User Agent, Service Provider/Service Provider Agent or TFNA's RND data submissions/updates/queries, and the generation of receipts regarding each RND data submission/update/query
- Maintain data integrity
- Offer a web interface and allow for automated data input for RND data needed for the processing of User/User Agent queries and Service Provider/Service Provider Agent and TFNA data queries and report submissions
- Accommodate automated data upload via secure FTP from Service Providers/Service Provider Agents and the TFNA when transmitting data for their monthly disconnected numbers report submissions
- Accommodate automated data input and output via secure FTP or RESTful API to Users/User Agent when transmitting RND Query Requests and RND Query Responses

[21] Note: This transaction report can be used for no-charge billing, can be used to create transaction summary and detailed reports.

- Accommodate the ability for a User/User Agent or the FCC to perform a Web GUI RND Query Request of up to 50 individual TN's at a time.
- Accommodate the ability for a Service Provider/Service Provider Agent or the TFNA to perform a Web GUI data upload of up to 50 TN's at a time
- Be capable of generating an RND Query Response within two (2) seconds 95% of the time over any 12-month period when a Web GUI Query Request has been submitted
- Be capable of generating an acknowledgement to the Service Provider/Service Provider Agent and TFNA data submission within two (2) seconds 95% of the time over any 12-month period when Web GUI data has been submitted
- Support Client access to secure RND data, as appropriate for that type of user, with a unique User ID and password
- Provide Service Providers/Service Provider Agents and the TFNA with the ability to query and retrieve their data on a read-only basis and shall have the ability to download the query report data to an Excel™ or .CSV format.

3.2.1 Initial RND Data Upload

The effectiveness of the RND depends upon comprehensiveness of the data that it will contain. Thus, the RND will become more comprehensive over time. The initial establishment of the database will need to include a volume of data that will provide an initial comprehensiveness so that Users/User Agents will experience value. Thus, the RNDA:

- Shall have the ability to receive and load, into the RND, the initial TN data file(s) of Permanently Disconnected TNs from Service Providers/Service Provider Agents and the TFNA. These "seed" files will include Permanently Disconnected TN data beginning on the first date of data collection, as determined by the FCC.[22]

- Shall have the ability to receive multiple files per Service Provider/Service Provider Agent and the TFNA.[23]

- Shall only retain the TN record that has the most recent Permanently Disconnected Date if the initial file(s) contains duplicate records for a particular TN in the RND. The initial set of data when the RND is available shall have only one instance of a TN record. TN history will not be available until the monthly Service Provider/Service Provider Agent and TFNA file uploads begin.

3.3 System Location

RND system/servers shall be in the cloud with a FedRAMP-compliant cloud service provider that has been assessed and authorized through the FedRAMP[24] and FCC authorization processes, and has agency-approved Authority to Operate. The RND servers shall be within the continental United States, but location within the continental United States is at the discretion of the contractor.

3.4 System Data

RND data and information shall be stored in the RND in accordance with the categories and formats that correspond to those outlined in this TRD, FCC18-177 and/or as may be defined in the future by FCC directives and the appropriate stakeholders (*e.g.,* INC/RND system user group).

---

[22] See FCC 18-177, ¶41.

[23] Service Providers/Service Provider Agents and the TFNA may elect to provide multiple files of data or a single file of data.

[24] *See* www.fedramp.gov.

3.4.1 Data Integrity

The RNDA shall take commercially reasonable steps to ensure that all Service Provider/Service Provider Agent and TFNA data provided is accurately appended into the RND. Furthermore, the RNDA shall ensure that the RND Query Response provided to Users/User Agents is accurate based upon the User/User Agent RND Query Request.

3.4.2 Confidential Treatment

All Client-specific data submitted to the RNDA, in any form, shall be treated as confidential. All confidential data or proprietary information shall not be accessible by the public on the RNDA web site, or published by the RNDA.

3.4.3 Automated Submittal

The RNDA shall implement in the RND, at a minimum, the data interface protocols outlined above in Section 2.15.1 for Service Provider/Service Provider Agent and TFNA to submit monthly permanently disconnected number data. Except as noted, the RND shall offer a web interface and/or allow for automated data input via EFT/secure FTP for appending of the RND, as well as support data entry via the system GUI (manual input and file upload/download). The EFT/secure FTP capabilities shall permit Service Providers/Service Provider Agents and the TFNA to submit data in a predetermined format, per the forms from the relevant guidelines for the RND data, which the RNDA shall then use to initiate automated processing within the RND.

3.4.4 System Reports

3.4.4.1 Query User/User Agent RND System Report

At a minimum, the RND shall be capable of producing the following report and shall be downloadable in an Excel™ or .CSV format.

- Audit report consisting of:
    - Query Originator
    - RND Query Request date/time
    - Number of TN(s) queried,
    - Query Response date/time
    - Number of ”yes”, “no”, and “no data” RND Query Responses

3.4.4.2 Service Provider/Service Provider Agent and TFNA Data Input System Report

At a minimum, the RND shall be capable of producing the following report and shall be accessible via downloadable in Excel™ or .CSV file format:

- Report listing the dates of disconnected number report submissions of a Service Provider/Service Provider Agent or the TFNA based upon query of date range.
- Audit report consisting of:
    - Date/time RNDA received data for update
    - Company Identifier from which the data is received
    - RND update date/time
    - User ID that updated the RND
    - TN updated
    - TN Disconnect Date

3.5 System Maintenance

Regularly scheduled maintenance shall be included in a System Maintenance Plan and shall require prior approval of the FCC. The details of a proposed system maintenance schedule shall be provided in the RNDA's System Maintenance Plan. All scheduled maintenance activities shall occur during non-core business hours, shall not occur during the required disconnected number report submission period, and shall not exceed a four (4)-hour period unless approved by the FCC.

3.6 System Security

The RNDA shall maintain and enforce system safety and physical security procedures in accordance with the *FCC Cyber Security Program* (Reference 1). The RNDA shall maintain confidential and proprietary information and institute any physical and safety procedures required. The details shall be provided in the RNDA Security Plan. Any security breach shall be documented and reported to the affected Client and the appropriate regulatory authority as soon as the RNDA is aware the breach occurred.

Following contract award, the RNDA shall prepare an RNDA Security Plan following, as appropriate, the National Institute of Standards and Technology (NIST) *Guide for Developing Security Plans for Federal Information Systems* (Reference 6).

3.7 RND System Access

The RNDA shall develop and maintain an online RND System Access Profile application process for a prospective system user to request a unique system User ID and password that distinguishes one system user from another. The RND System Access Profile application shall contain at a minimum the contact information (mailing address, email address, phone number) of the system user, the billing information (as appropriate), and the type of system user access. A system user applicant shall have the ability to select one of the four types of system user access that pertains to that system user (*i.e.,* User/User Agent, Service Provider/Service Provider Agent, Toll Free Number Administrator (TFNA), or FCC). Each type of system user shall have a separate system profile type that determines the capabilities and functionalities available to that type of system user. System user Profiles shall allow system users to specify additional contacts that will allow system responses to be sent to multiple system users (*e.g.,* If a Service Provider Agent submits disconnected number data on behalf of Service Provider, the Service Provider Agent shall have the ability to specify additional email contacts for that Service Provider so that both the Service Provider Agent and Service Provider will receive confirmation of submission emails). Following are the four types of system user profiles:

User/User Agent – In addition to system user contact information, the User /User Agent Profile application shall require the applicant's billing information and information necessary for the creation of a unique Company Identifier (assigned by the RNDA). The User/User Agent Profile shall be used to ensure that User/User Agent system users are limited to querying the RND with a telephone number and date, and subject to their contracted query levels (*e.g.,* system users from the User A company can submit unlimited queries to the RND because User A company pays a flat monthly fee to do so, while system users from User B company are restricted to a certain quantity of queries to the RND per month because User B company pays a tiered monthly fee to do so).

Service Provider/Service Provider Agent – In addition to system user contact information, the Service Provider/Service Provider Agent Profile application shall require the applicant's unique Company Identifier which may be either self-assigned by the Service Provider/Service Provider Agent or assignable by the RNDA at the Service Provider/Service Provider's Agent's option. For Service Provider Agents, the application also shall require the company identifiers of the Service

Providers for which the Service Provider Agent will submit monthly disconnected number data. The Service Provider/Service Provider Agent Profile shall be used to ensure that Service Provider/Service Provider Agent system users are limited to reviewing their own company's data (*e.g.,* system users from Service Provider A can only access data that a system user from Service Provider A has provided, and cannot access any data that a system user from Service Provider B has provided).

Toll Free Number Administrator (TFNA) – In addition to system user contact information, the TFNA Profile application shall require the applicant's unique Company Identifier (assigned by the RNDA). The TFNA Profile shall be used to ensure that TFNA system users are limited to reviewing only the disconnected toll free number data that the TFNA has submitted, and not User/User Agent queries or Service Provider/Service Provider disconnected US geographic telephone number data submitted.

FCC -- The FCC Profile shall be used to ensure that FCC system users are able to query the RND for compliance or verification purposes in the same manner that a User/User Agent can, but at no charge. The FCC Profile shall also be used to ensure that FCC system users are able to review disconnected number data submitted by any and all Service Provider/Service Provider Agent system users or TFNA system users. Such broad access is necessary for the FCC to oversee the performance of the RNDA and ensure Service Provider and TFNA compliance.

3.7.1 Logon System Access and Profiles

3.7.1.1 User/User Agent Logon System Access

The RND system shall be able to support appropriate access to the RND with a unique User ID and password (i.e., Logon Credentials) upon receipt and approval by the RNDA of a User/User Agent Profile request form. The RNDA shall establish an approval process for establishing the Logon Credentials of Users/User Agent system users. Access is initiated upon receipt by the RNDA of a completed Logon Credentials request form having the proper written approvals from within the requesting User organization, or online approval from the Primary Contact for that company.

For User Agents querying the RND on behalf of individual Users, the User Agent must indicate its authorization to query the RND on behalf of the User company through its possession of a Letter of Authorization (LOA) for each separate User company registered under the User Agent's Profile. Upon request by the RNDA, the LOA must be provided to the RNDA via email. The LOA must be on the User's company letterhead and contain 1) the company identifier of the User for which the User Agent is acting on behalf of, 2) the LOA must be signed by the User, and 3) the LOA must be dated. The RNDA shall establish and publish a validation process for establishing or transitioning a User Agent's authorization to query the RND on behalf of a User. This process should enable efficient and timely resolution by User Agents for any User Agent Profile conflicts.

3.7.1.2 Service Provider/Service Provider Agent Logon System Access

The RND system shall be able to support appropriate access to the RND with a unique User ID and password upon receipt and approval by the RNDA of a Service Provider/Service Provider Agent Profile request form. The RNDA shall establish an approval process for establishing the Logon Credentials of Service Provider/Service Provider Agent system users. Access is initiated upon receipt by the RNDA of a completed Logon Credentials request form having the proper written approvals from within the requesting Service Provider organization or online approval from the Primary Contact for that company.

For Service Provider Agents reporting on behalf of individual Service Providers, the Service Provider Agent must indicate its authorization to submit disconnected number reports or updates to the RND on behalf of the Service Provider through its possession of an LOA for each separate company registered under the Service Provider Agent's Profile. Upon request by the RNDA, the LOA must be provided to the RNDA via email. The LOA must be on the Service Provider's company letterhead and contain 1) the company identifier for the Service Provider for which the Service Provider Agent is acting on behalf of, 2) the LOA must be signed by the Service Provider, and 3) the LOA must be dated. The RNDA shall establish and publish a validation process for establishing or transitioning a Service Provider Agent's authorization to submit disconnected number reports or updates to the RND on behalf of a Service Provider. This process should enable efficient and timely resolution by Service Provider Agents for any Service Provider Agent Profile conflicts.

3.7.1.3 TFNA Logon System Access

The RND system shall be able to support appropriate access to the RND with a unique User ID and password upon receipt and approval by the RNDA of a TFNA Profile request form. The RNDA shall establish an approval process for establishing the Logon Credentials of TFNA system users. Access is initiated upon receipt by the RNDA of a completed Logon Credentials request form having the proper written approvals from appropriate personnel within the TFNA or online approval from the Primary Contact for that company.

3.7.1.4 FCC Logon System Access

The RND system shall be able to support appropriate access to the RND with a unique User ID and password upon receipt and approval by the RNDA of an FCC Profile request form. The RNDA shall establish an approval process for establishing the Logon Credentials of FCC system users. Access is initiated upon receipt by the RNDA of a completed Logon Credentials request form having the proper written approvals from appropriate personnel within the FCC or online approval from the Primary Contact for that company.

3.7.2 Logon System Approval

After access approval, the RNDA shall assign the unique User ID and password with the appropriate security level corresponding to the system user's System Access Profile type.

3.7.3 Logon System Security Level

The system user's System Access Profile type sets the correct level of record access and system capabilities. For any forms requiring a signature, a valid User ID and password shall be considered tantamount to a signature.

3.7.4 Logon System Password

After the User ID is initialized, the system user shall be informed of the User ID activation and password via email or other notification.

3.7.5 Logon Profile and Contact List Maintenance

The RNDA shall maintain the ability to reach all registered system users by requiring system users to review and update their contact information and billing information semi-annually. The RNDA's contact list shall be automated and allow contact by e-mail.

3.7.6 Logon System Problems

RND system users experiencing problems in obtaining appropriate access to the RND via initialized Logon Credentials shall contact the RNDA for resolution. The RNDA shall resolve all Logon Credential problems within one business day.

3.7.7 Active Access Permissions and Primary Contacts

The RNDA shall exercise appropriate control over access to all records, and shall ensure that User/User Agents, Service Provider/Service Provider Agents, TFNA and FCC system users are only allowed access to the data appropriate to their respective permissions.

The RND shall provide the ability for each system user type (*i.e.,* User/User Agent, Service Provider/Service Provider Agent, TFNA and FCC system user) to query and download a report of all active system users associated with the system user's company (*e.g.,* a system user can query and download a list of all active system users associated with that company), without having to request such information from RNDA personnel. Further, the RNDA shall ensure that each company with RND system access has a Primary Contact designated for that company. Once the Primary Contact has a system User ID and password, the Primary Contact shall then be responsible for approval or denial of additional RND systems users for that company.

3.7.8 Password Changes

All User ID passwords shall be changed every 180 days. The RNDA shall establish a system user guide that addresses the Primary Contact's responsibility to notify the RNDA if an individual with Logon Credentials ends employment with the company or no longer needs access to the RND system. Upon such notification, the RNDA shall immediately remove or disable the Logon Credentials.

3.7.9 Locking/Unlocking Accounts

The RNDA shall establish criteria for locking system user accounts consistent with industry practices, such as the National Institute of Standards and Technology's *Digital Identity Guidelines* (Reference 14). The RNDA shall establish a policy regarding unlocking accounts, including verification that there is not a threat to system security and integrity. The RNDA shall implement the policy for all accounts meeting the stated guidelines.

3.7.10 Unauthorized System Access

In the event the RNDA becomes aware of an unauthorized access to the RND or RND associated data (*e.g.* account information), the RNDA shall immediately:

- Notify the FCC and the applicable system user(s) by email.
- Report to the NANC or its designee that a breach has occurred and that the affected party has been notified.
- Investigate the unauthorized access
- Provide the FCC and affected system users (subject to reasonable access, security, and confidentiality requirements) and their respective designees with reasonable access to all resources and information in the RNDA's possession as may be necessary to investigate the unauthorized access.

The FCC or its designee shall have the right to conduct and control any investigation relating to the unauthorized access as it determines is appropriate.

Complete information describing the security mechanisms used to prevent unauthorized access to its computers and telecommunications equipment, including internal policies, procedures, training, hardware and software, etc., will be furnished in the RNDA's Security Plan.

Upon completion of such investigation, the RNDA will provide options and a recommendation to prevent such unauthorized access and related implementation schedules for approval by the NANC or its designee.

3.8 System Inspection

Subject to the RNDA's reasonable access, security, and confidentiality requirements, the FCC or its designee upon notice to the RNDA, shall have the right to inquire about the safety/security functions of RND in the cloud application. The FCC or its designee, with or without notice to the RNDA, shall have the right to make visits to the RNDA to review safety/security requirements.

If any of the safety and physical security procedures as stated in the selected Offeror's proposal are not implemented and maintained throughout its Term of Administration, or any safety and physical security procedures related to the RND do not comply with those specified, the RNDA shall be deemed noncompliant. The RNDA shall implement corrective measures of noncompliance within ten (10) calendar days of notice of noncompliance. Failure to correct such noncompliance within ten (10) calendar days shall subject the contractor to termination of the contract for default.

The RNDA shall: (1) implement corrective measures, and (2) give notice of such implementation to the FCC or its designee. The FCC or its designee may make one (1) or more follow-up visits, as necessary, to confirm the deficiency has been rectified. The FCC or its designee's rights under this paragraph shall not in any way limit the FCC or its designee to visit the RNDA for reasons other than a safety/security visit.

System inspections may include, without limitation, the system or system components located at: RNDA or subcontractor facilities; telecommuting employees of the RNDA or subcontractor(s); RNDA or subcontractor maintenance organizations; or employees of the RNDA or subcontractor(s) on traveling status with access to the RND.

3.9 System Report Administration and Distribution

All reports generated or provided by the RND shall be treated as confidential or proprietary. The RND shall be capable of generating and distributing reports upon request, to all requesting Service Providers/Service Provider Agents, Users/User Agents, the TFNA and/or the FCC or its designee who are entitled to receive reports. The full set of reports shall be described in the RNDA's Management Reporting Plan. These reports shall include but may not be limited to the following:

- Service Provider or TFNA reporting compliance
- Service Provider or TFNA reporting Audit information
- Query information used in support of TCPA compliance

All Client specific reports of data shall be available to the authorized Service Provider/Service Provider Agent, User/User Agent, the TFNA and/or the FCC or its designee and accessible electronically through the secure GUI. All individual, Service Provider/TFNA/User-specific data submitted to the RNDA in any form, shall be treated as confidential. Any data that contains proprietary Service Provider/TFNA/User information shall not be accessible by the public on the RNDA web site or published by the RNDA.

The RND shall be responsible for the accuracy of report contents. Reports generated by the RND shall be capable of being distributed and updated automatically. The report distribution system shall support an email distribution list for signup for updated report notification.

The RNDA shall distribute via the RNDA web site all summaries and comprehensive reports made known to the RNDA or produced by the RNDA or its affiliate subcontractor(s) performing RNDA duties in part or whole. Reports shall be distributed by email when requested. Such reports shall be downloadable in a machine-readable form using standard word processing and spreadsheet programs, as appropriate.

3.10 Help Desk

The RNDA shall maintain a Help Desk that is accessible during the RNDA's regularly scheduled business hours. Among other functions, the Help Desk shall be available to assist Service Providers/Service Provider Agents, the TFNA, Users/User Agents, or the FCC with the input/output and the interpretation of system-generated reports. The RNDA Help Desk shall:

- Provide and maintain a toll free phone number to assist with interpretation of any system problem or inquiries related to the RND.
- Open trouble tickets as needed (see Section 3.10.4).
- Assist Clients and prospective Clients with profile creation or profile updates, and accessing reports.
- Answer RND specific questions from Service Providers/Service Provider Agents, the TFNA, Users/User Agents and other entities as needed, and provide information on where and how to obtain more information about the RND on the RNDA web site.

3.10.1 Contact

The toll free telephone number for the Help Desk shall be posted on the RNDA and RND web site along with other relevant contact information to help system users or prospective system users. The RNDA shall provide mechanisms (*e.g.*, web site, voicemail, e-mail) to be accessible on a 24-hour basis.

With e-mail, the RNDA shall have the capability of transmitting and receiving e-mail messages with and without attached files. The RNDA shall provide "firewall" protective screening of all incoming e-mail messages and attachments based on a security profile established by the RNDA and approved by the FCC or its designee. Additionally, the RNDA shall provide virus protection software on all devices that receive e-mail. The RNDA shall maintain the most recently updated version of virus software as defined by the software provider.

3.10.2 Help Desk Referrals

Response to system user or prospective system user inquiries for assistance shall include, where appropriate, referral to an RNDA Subject Matter Expert.

3.10.3 Help Desk Actions

Any frequently asked questions (FAQs) and their answers shall be added to the FAQ page on the web site on at least a monthly basis. Responses shall be provided within one business day of the request being sent to the RNDA.

3.10.4 Help Desk Trouble Ticket Tracking and Reporting

The RNDA Help Desk shall track and resolve trouble tickets. The RNDA Help Desk shall:

- Open a trouble ticket for each reported problem with the RND, the web site, voice mail or e-mail.

- Require that each trouble ticket be time stamped with minute accuracy and stored for recall for two (2) years.
- Use the time stamped on the trouble ticket as the time for the start of the out-of-service period when an out-of-service condition exists; when the out-of-service condition has been cleared and the originator of the trouble ticket notified, use the time stamped on the last update of the trouble ticket shall be used as the end of the out-of-service period.
- Notify the originator of the trouble ticket of the disposition of the problem once the trouble ticket is closed.
- Summarize the quantity and type of trouble tickets opened and closed during the year in the Annual Report.
- Monthly summary of trouble tickets opened, closed, and resolution to be available to the FCC or its designee.
- Report other problems that, while not related to the RND, the web site, voice mail or email, are likely to be visible and impact multiple users.

3.11 System Tutorial

Upon accessing the system for the first time, authorized system user groups shall be provided the option of using a tutorial about: various system functions available, the type of data in the system, and protection of the confidential data. The tutorial shall be tailored to particular system user groups. The RNDA shall create the tutorial with input from the FCC or its designee. The tutorial shall be available to system user groups at any time after their initial use of the system.

3.12 System Generated Notifications and Customized Notifications

The RND shall support an email distribution list that registered RND users can apply to and receive system generated notifications. Such an email distribution list may be used to send a general notice to registered RND system users.

The RND shall allow registered RND system users to customize notices by selecting the categories of notices they want to receive, such as:

- Instructions for system users or other general web site users to subscribe to lists posted on the RNDA web site
- Topic specific notifications
- General broadcast of system availability or maintenance
- System user education opportunities
- New items on the web site
- New personnel announcements

3.13 System Testing and Results

Prior to any new system turn up or any new system functionality and feature implementation turn up, the RNDA shall provide and maintain a test bed for testing of the RND in anticipation of the system acceptance test, as well as future system changes, and shall provide a System Test Plan to the FCC for the initial acceptance test of the RND. This plan shall contain the selection criteria for system users to participate in system testing and the timeline and specific RND elements to be tested. The System Test Plan shall follow the format, where applicable, of *ISO/IEC/IEEE International Standard - Software and systems engineering — Software testing —Part 3: Test documentation (*Reference 2).

The RND shall be subject to any system test deemed appropriate by the FCC to ensure the efficacy of the guidelines, any standards that are referenced or cited in any of the documents in Section 10 of this document or any standards that are offered in contractor's proposal (*e.g.,* the Internet Engineering Task

Force (IETF) interface standards for Internet Protocol (IP), or numbering plan standards, like ITU-T Recommendation E.164).

The testing will ensure the efficacy of the, interfaces and standards. The RNDA shall develop and implement a System Acceptance Plan following the format, where applicable, of *ISO/IEC/IEEE International Standard - Software and Systems engineering –Software testing – Part 3: Test documentation* (Reference 2).

Upon completion of the RND acceptance test, the RNDA shall inform the FCC of the results. These results shall be generalized and made available to prospective system users.

Final approval of the RND shall be dependent on successful execution of the System Acceptance Plan, which shall include a System Test Plan. The System Acceptance Plan shall be submitted to the FCC within 30 days of contract award and shall be successfully completed within 90 calendar days of the contract award.

3.14 System Disaster Recovery and Costs

A disaster recovery process shall be developed to restore the RND within two (2) business days. The RNDA shall develop and implement a detailed Disaster/Continuity of Operations Plan, following the format, where applicable, of *NFPA 1600® Standard on Continuity, Emergency, and Crisis Management* (Reference 3) 60 days following contract award. In the event of a disaster, the RNDA shall cover all costs associated with rebuilding or recovering the applications systems, records, and related information that existed prior to the disaster.

3.15 System Backup

The RNDA shall initiate and maintain a backup process that ensures that the data contained in the RND can be restored as needed. RND backup information shall be generated at least daily. The RNDA shall keep a full backup of the web, application, and database servers using an FCC-approved web services provider, where the data will be retained and accessible if necessary.

3.16 System and Equipment Inventory

Inventory data on personal computer equipment shall be reported as part of the RNDA's annual reporting requirements, as well as any upgrades or replacements, including the license numbers of any Commercial Off-the-Shelf (COTS) software.

3.17 Implementation of System Documentation Plan

The RNDA shall have in place the System Documentation Plan, pursuant to section 7.14 prior to RND system implementation.

3.18 Reassigned Number Database (RND) Transfer to Successor

The RNDA shall transfer to the FCC or a successor, in the case of termination, or at the expiration of the Term of Administration, all intellectual and physical property, accounts and web sites developed with funding from this contract and used in conjunction with the RND/RNDA. This means that everything transfers, including all items attached to the RND. Any other intellectual or physical property or contracts associated with the RNDA day-to-day operations shall transfer. This shall include but not be limited to:

- RND and all its accounts and supporting documentation
- Cloud-based applications and other software
- Test bed system(s)
- Interface specifications and supporting documents

- All property associated with RND/RNDA
- All disconnected numbers and disconnect date records
- Also see the RND Transition Plan

The RNDA shall provide to the FCC a detailed RND Transition Plan that provides for an efficient and orderly transition, which includes a list of items that are subject to transfer at the end of its term. This Transition Plan shall follow the format, as applicable, of *Software Transition Plan (STrP)* (Reference 4). The RNDA shall file the Transition Plan with the Contracting Officer once its RND has been accepted. Thereafter, the RNDA shall update the Transition Plan annually, and provide it to the FCC.

3.18.1 Transfer Efficacy

Transfer of property shall be performed in such a manner as to ensure an efficient and orderly transition of the RND, cloud-based applications and any associated property to a successor's environment in a fully operational state without service interruption to any Client.

3.18.2 System Software Source Code Escrow

The FCC shall be the custodian of a copy of the RND source code and any other code necessary to make the software and system executable, including any documentation. The RNDA shall provide the FCC with copies of all documentation specified in the System Documentation Plan.

3.18.3 Property Inventory and Transfer

Any property related to the RND shall transfer with lien-free title to the FCC or the FCC's designee, without charge. Inventory data (models, serial numbers and descriptions) on any property shall be reported as part of the RNDA's annual reporting requirements, as well as any upgrades or replacements, including the license numbers of any commercial item software.

3.18.4 Technical Support

After the period provided in the services continuity clause (*Federal Acquisition Regulation (FAR) Section 52.237-3)* (Reference 12), if requested, the RNDA shall provide up to 45 business days (over a six (6)-month period) of technical support to ensure a smooth transition of the system.

3.19 Tools

The RND shall maintain the applications and tools necessary for system users to access and use the system to perform the applicable tasks and functions.

3.19.1 RND Query Request and Data Submission Processing

The RND and tools shall provide real time access to RND data. The RND shall support standard electronic filing capabilities (*e.g.,* secure FTP/RESTful API).

3.19.2 Federal Requests/Directives/Orders

The RNDA and/or a system application shall be capable of responding to a request by the FCC for assistance and/or advice on an RND issue that may affect existing processes and procedures used by Service Providers/Service Provider Agents, TFNA, and Users/User Agents. Upon an FCC Directive or Order, the RNDA shall post on the RNDA web page the impact of the Directive or Order upon the RND or Service Providers/Service Provider Agents, TFNA, and/or Users/User Agents.

3.19.3 Contact Information

The RNDA shall record any contact information provided by Clients. The record shall contain the name, address, e-mail address, telephone number, company name, title and area of responsibility, and the date

the record was updated. The database shall be capable of report generation using any of the entered fields for Clients, but such reports can only be accessible by the RNDA.

3.20 Web Site

The RNDA shall provide and maintain an Internet web site that provides the functionality and information necessary to serve its Clients (*e.g.,* allow Service Providers/Service Provider Agents and TFNA to submit monthly reports securely, and allow Users/User Agents to query the database).

3.20.1 Web Site Content

The RNDA web site shall contain links to applicable industry guidelines, secure access to the RND for registered system users, and other information to assist its Clients. At minimum, the RNDA web site shall contain the following content:

Category	Content
1. RNDA Information	• RNDA general information • All relevant staff contact names, updated as necessary • Telephone numbers • Facsimile numbers • E-mail addresses
2. Secure Access to the RND	• Access to the RND for registered Users/User Agents to query the RND • Access to the RND for registered Service Providers/Service Provider Agents and the TFNA to submit reports
3. INC guidelines	• ATIS website
4. RNDA Reports	• List of RNDA Reports concerning the RND • Annual report (downloadable in a machine-readable format as appropriate) • FCC and Metrics Reports, as required
5. Tools	• Various tools designed to assist Clients and other web site visitors, such as Frequently Asked Questions (general and Client-type specific, as needed), a Glossary, Quarterly Tips, Password Reset, new Service Provider/Service Provider Agent and TFNA Registration, new User/User Agent Registration, etc.
6. Change Orders	RNDA to ensure the change orders are on the website.
7. Other Documents	• Reporting procedures and templates • Querying procedures and templates • User Guide for Service Providers/Service Provider Agents and the TFNA • User Guide for Users/User Agents querying the RND

Category	Content
	• Secure FTP/RESTful API Registration • Problem Resolution Process
8. Complaints, Comments, Suggestions	Ability to submit and track online forms to submit a complaint, comments or concerns, or suggested enhancements for the web site or the RND
9. Dashboard	A real-time overview of any service problems with the RND, including its outage status, system users impacted

3.20.2 Content Posting and Updates

The web site shall contain current information. New information and documentation shall be posted to the RNDA web site within one (1) business day of its release. Information contained on the web site shall be updated within one (1) business day of any change or document release.

The web site shall provide RND help information that is constantly being improved, added to, and updated. This knowledge base of help information and Client-specific FAQs content shall be updated as needed.

3.20.3 Web Site Design

The RNDA web site shall be reliable and be able to quickly fulfill reasonable user expectations. The RNDA's web site shall be designed and maintained to ensure its accessibility according to the following principles:

- Maintain a RNDA web site easily accessible by all users
- Allow web site pages to be navigated by keyboard
- Provide alternative methods to access non-textual content, including images, scripts, multimedia, tables, forms and frames for users who do not wish to display them
- Use accepted web site features (*e.g.*, drop down menus) to provide information about the purpose and function of web site elements
- Provide a search engine to facilitate site navigation

3.20.4 Availability and Access

The RNDA web site shall be available 24 hours a day, 7 days a week. The web site shall be able to support a minimum of 1,000 simultaneous users initially, with an average holding time of 0.5 hours, to ensure that no web site user's experience is degraded when accessing or attempting to access the web site. The RNDA shall review at least monthly the first year and semi-annually thereafter the quantity of simultaneous users and shall have the flexibility to adjust the support accordingly. The RNDA shall make such adjustments on an as needed basis.

3.20.5 Web Site Responsiveness

The RNDA shall provide rapid response when users are accessing the web site. The RNDA shall provide a web site such that will allow users the ability to view the complete web site home page in less than 3 seconds, 95% of the time over any 12-month period.

If a user is experiencing greater than 8 seconds to view the complete web site home page, the RND system shall have the capability to sense this condition. The RNDA shall open a trouble ticket to investigate whether the problem is between the web site and the Internet Service Provider (ISP) or is in the RND system. If the user reports to the Help Desk a problem with accessing information on either the

web site or the RND system, a trouble ticket shall be initiated to determine if an "out of service" condition exists.

3.20.6 Out-of-Service

The RNDA web site and the RND system shall be operational 99.9% of the time over any 12-month period, excluding scheduled maintenance. The RNDA's inability to deliver services at this level shall be deemed "out of service." This figure excludes problems due to the user's network or equipment. All scheduled maintenance activities shall occur during non-core business hours, shall require prior approval of the FCC, and shall not exceed a four-hour period unless approved by the FCC.

If any "out of service" condition exists cumulatively for two (2) hours (or more) in any 24-hour period, as evidenced by a user trouble report to the RNDA, the RNDA shall provide an out-of-service credit to the FCC in an amount equal to 1/30th of the previous month's charge for the month in which the outage occurred.

The RND system shall be capable of "pinging" its ISP(s) every five (5) seconds to confirm that the round-trip latency is less than or equal to ten (10) milliseconds. If the latency is greater than ten (10) milliseconds, the connectivity between the web site and ISP(s) shall be considered out of service and a trouble ticket opened.

3.20.7 Out-of-Service Notification

The RNDA shall be the point of contact for system recovery. The RNDA shall be capable of distributing system status and outage reports to all registered Clients. All scheduled maintenance activities shall be approved in advance by the FCC prior to commencing the activity. Once the FCC has approved the scheduled maintenance activity, the RNDA shall provide notification to all registered Clients as to when the activity will begin and end, as well as the impact on the Clients. In addition, the RNDA shall notify and report to all Clients and the FCC of an unscheduled system shutdown or failure.

3.20.8 Web Site Privacy

Web site privacy shall be monitored every time content and transaction functionality is added or changed to avoid any risk of exposing the web site to privacy risks and inappropriate access to the content.

3.20.8.1 Privacy Management

Privacy management shall include the rules that govern the collection, use, retention, and distribution of data. It shall address the privacy needs of Clients by assessing the risks to confidential data; managing the implementation of privacy policies and associated procedures; ensuring on-going compliance; monitoring developments, accommodating changes, and raising awareness within the RNDA's organization; and training RNDA staff.

3.20.8.2 Privacy Compliance

The RNDA's privacy practice shall contain details listing the compliance with the Gramm-Leach Bliley Act of 1999 regarding regulating the privacy of personally identifiable, non-public financial information in the United States. The RNDA shall prominently display its privacy statement explaining RNDA's information handling practices on its web site.

3.20.8.3 Privacy Breaches

The RNDA shall monitor web site access to ensure that identified privacy practices are not compromised in any fashion. Any web site data privacy breach shall be documented and reported to the affected user and the appropriate regulatory authority as soon as the RNDA is aware the breach occurred.

Section 4: Reporting

The following section discusses the reports requirements for the RND. RNDA reporting shall take the following forms:

- an update to a table or document on the RNDA secure and/or non-secure web site as applicable
- an electronic attachment to or notification of posting via an e-mail distribution list

The RNDA shall provide regular reports as defined in this section on specified RND criteria.

The applicable report frequency shall be provided and/or made available, to the FCC or its designee as appropriate, annually, quarterly, and monthly, subject to change as deemed necessary.

The applicable report frequency shall be provided and/or made available to, Service Providers/Service Provider Agents, TFNA, and User/User Agents as appropriate, annually, quarterly, and monthly, subject to change as deemed necessary.

The report format shall include a combination of charts, graphs, and/or narratives, shall be subject to change, and shall include any other information the FCC or its designee deem necessary.

4.1 Annual Reports

The RNDA shall publish an Annual Report on the status of the RND including aggregated activity of User, Service Provider, TFNA, and the Data administered by the RNDA. The report shall be published during the first quarter of each year. The annual report shall be made available through the RNDA secure web site.

The Annual Report shall contain at a minimum, but not be limited to:

- Brief description of the RND and the RNDA
- Historical trends
- Highlights/significant milestones reached during previous year
- System and performance metrics
- Status of required transferable property
- Industry issue identification/feedback
- Volume of reports produced for regulatory agency, Users, TFNA, and Service Providers
- Rolling month over month RND performance report (Up/Down time)
- Rolling month over month User metrics (Database queries)
- Rolling year over year User metrics (Database queries)
- Rolling month over month Service Provider and TFNA metrics (Database updates)
- Rolling year over year Service Provider and TFNA metrics (Database updates)
- Rolling month over month total disconnected numbers
- Rolling year over year total disconnected numbers
- Rolling month over month report on staffing
- Rolling month over month report on the number of ad hoc reports generated
- Self-Assessment of the RNDA
- Complaints received by the RNDA
- Technical Requirements Document updates

4.2 Requests for Additional Reports

The RNDA may also be requested to produce additional reports as needed by authorized entities.

4.3 Reference Documentation

The RNDA shall maintain and make readily available an addendum of reference documentation to assist interested parties. The list shall include the most recent version of all applicable guidelines and all RNDA-related regulatory directives and requirements. This addendum shall be posted on the RNDA web site and updated as needed.

4.4 Monthly Performance Report

The RNDA shall provide monthly reports to the FCC or its designee on the performance of the RND. The monthly Performance Report shall, at a minimum, include:

- Percent of scheduled time the RND was available in the month
- Hours and minutes of potential RND availability
- Hours and minutes of actual RND availability
- Number of instances of RND scheduled unavailability
- Hours and minutes of RND scheduled unavailability
- Number of instances of RND unscheduled unavailability
- Hours and minutes of RND unscheduled unavailability.

The monthly RND Performance Report shall be posted to the RNDA secure and/or non-secure web site as appropriate.

4.5 Monthly Trouble Tickets, Phone Calls and Change Orders Report

The RNDA shall provide monthly reports to the FCC or its designee on trouble tickets, phone calls, and change orders. At a minimum, the following is a list of reports to be provided:

- Quantity of trouble tickets opened, closed and pending resolution, by type of issue (*e.g.,* system performance, web site, system user error, other)
- Trouble ticket mean time to repair (MTTR)
- Listing of each trouble ticket with its status
- Quantity of phone calls received, and the quantity of phone calls not returned within 24 hours
- Quantity of change orders submitted, awaiting approval, approved but awaiting implementation, approved and implemented, or denied (if applicable). A brief description shall be provided for each change order.

4.6 Monthly Reports

At a minimum, the RNDA shall produce the following reports to the FCC or its designee:

- Rolling month over month RND performance report (Up/Down time)
- Rolling month over month User metrics (Database queries)
- Rolling month over month Service Provider and TFNA metrics (Database updates)
- Rolling month over month total disconnected telephone numbers
- Rolling month over month report on staffing
- Rolling month over month report on the number of ad hoc reports generated

4.7 Quarterly Report

At a minimum, the RNDA shall produce the following reports:

- Rolling month over month RND performance report (Up/Down time)
- Rolling month over month User metrics (Database queries)
- Rolling month over month Service Provider and TFNA metrics (Database updates)
- Rolling month over month total disconnected telephone numbers

- Rolling month over month report on staffing
- Rolling month over month report on the number of ad hoc reports generated
- Self-Assessment of the RNDA
- Complaints received by the RNDA

4.8 Semi-Annual Reports

The RNDA shall produce semi-annual reports of aggregated data that summarize the quantities of disconnected numbers reported each month during the previous six months, producing separate reports for disconnected US geographic and toll free telephone numbers.

The disconnected US geographic telephone numbers report shall at a minimum, identify the aggregated total of disconnected numbers reported each month and the quantity of Service Providers or reports submitted each month.[25]

The disconnected toll free telephone numbers reports shall at a minimum, identify the aggregated total of toll free disconnected numbers reported each month.

Such semi-annual reports shall be provided to the FCC or its designee and posted on the RNDA web site by the last business day of June and December of each year, unless otherwise directed by the FCC.

4.9 Dashboard

The RNDA shall provide a real-time dashboard where an overview of service can be viewed on the RND secure and/or non-secure web site as appropriate. This shall also provide an overview of service problems with the RND. The following are examples of viewable items:

- Last date that RND has been updated
- Status of the RND (scheduled/unscheduled outage)
    - Availability for Client query
    - Expected RND restoration time

4.10 Ad Hoc Reports

Upon request by the FCC, or its designee; the RNDA shall provide ad hoc reports concerning information contained in the RND system and performance of the system and its administrator.

4.11 Summary of RNDA Technical Reports

Following is a summary of the RNDA technical reports:

Name	Frequency	Audience
RND Annual Report	Annually (in first Quarter)	FCC or its designee
RND Performance Report	Monthly, Quarterly, Annually (in first Quarter)	FCC or its designee and posted on web site
User Metrics	Monthly, Quarterly, Annually	FCC or its designee
Service Provider & TFNA Metrics	Monthly, Quarterly, Annually	FCC or its designee; Service Provider, TFNA
Total Disconnected Numbers (Aggregated)	Monthly, Quarterly, Annually	FCC or its designee; Service Provider, TFNA
Staffing	Monthly, Quarterly, Annually	FCC or its designee

[25] No Service Provider-specific information shall be disclosed.

Ad Hoc Reports	Monthly, Quarterly, Annually	FCC or its designee
Trouble Tickets	Monthly	FCC or its designee
Phone Calls	Monthly	FCC or its designee
Change Orders	Monthly	FCC or its designee
Contact List Maintenance	Quarterly	RNDA
Customer Response Rates	Contingent, within one (1) business day; contingent and annual.	FCC or its designee
Self-Assessment	Quarterly, Annually	FCC or its designee
Unauthorized User Access	Contingent upon occurrence.	Affected Client and FCC or its designee
Privacy Breach	Contingent upon occurrence.	Affected Client and FCC or its designee
Complaints	Contingent, to be prepared within one (1) business day; Annually and quarterly	FCC or its designee
Technical Requirements Document Update	Semi-Annually	FCC or its designee, contingent upon change order implementation

Section 5: Audits

The RNDA shall be subject to FCC audits to verify their compliance with regulations and/or contractual provisions relating to all applicable areas of Disconnected Telephone Numbers administration.

5.1 Additional Obligations

The RNDA may be subject to other audit availability requirements under other clauses in the awarded contract.

5.2 Audit of the RNDA

The RNDA shall be subject to audits by the FCC or its designees that include but are not limited to the following:

- Compliance with any applicable industry guidelines
- Compliance with regulatory directives
- Conflict of Interest
- Neutrality
- RNDA operations and financial viability
- Record verification
- Facilities
- Security
- Log of all Client activity (including timestamps) such as Client uploads, system queries, system user updates, etc.

5.2.1 Staff Support

The RNDA shall provide the FCC and/or its designee access during normal business hours to the RNDA's staff and books, records, and supporting documentation relating to the RNDA function being audited.

5.2.2 Office Facilities

The RNDA shall provide office space, office furnishings, telephone and facsimile service, utilities, office-related equipment, and duplicating services that auditors may require to perform audits.

5.2.3 Audit Results

The RNDA shall make audit results available to the public in a limited manner that protects any confidential or proprietary information. The FCC and/or its designee shall receive a detailed summary of the audit results.

If any audit results in the RNDA being notified that it is not in compliance with any law, regulation, or requirement relating to its administration, the RNDA shall be required to take actions to correct any non-compliance as directed by the FCC and/or its designee.

5.2.4 Compliance

The RNDA shall present a corrective action plan to the FCC and/or its designee within 20 days after the receipt of the auditor's report. The RNDA shall report monthly or more frequently if appropriate, on the status of compliance efforts and notify the FCC and/or its designee upon completion of the corrective action plan. The RNDA shall bear the complete expense of compliance activities that arise out of the implementation of a corrective action plan. In the event that the RNDA does not meet its obligations, all remedies, including termination for default, are reserved to the FCC.

Section 6: Performance Monitoring, Measurements, Metrics

6.1 Performance Monitoring

The program and performance monitoring process shall include, but not be limited to, an internal, documented performance monitoring mechanism to be developed and implemented by the RNDA in accordance with performance measurements established in this Technical Requirements Document.

6.1.1 RNDA Client Feedback Survey

The FCC and/or its designee shall develop a formal Client feedback survey to permit all interested parties to provide performance assessment data and recommendations to the FCC and/ or its designee. The RNDA shall be responsible for hosting any online Client feedback survey.

6.1.2 RNDA Annual Operational Review

The RNDA shall undergo an annual operational review to be conducted by the FCC and/or its designee.

The operational review shall consist of a review of appropriate RNDA operations and facilities to ensure that the RNDA is performing its functions and responsibilities in accordance with the requirements of the contract. The RNDA shall ensure that all data provided to the group conducting the operational review adheres to all confidentiality requirements. The operational review shall at a minimum, address the following topics:

- Status of trouble tickets
- Status of Quality Assurance, Program Improvement Plan (PIP), and associated implementation management
- Status of security plans and disaster recovery activities
- Status of external relations and any special projects
- Status of reporting, compliance, and regulatory communications

- Status of the RNDA job aids, training videos, and other tools for the industry
- Status of job aids and tools for employees to ensure a knowledgeable workforce and external communication alignment

6.1.3 Program Improvement, Performance Problems, and Corrective Action

The RNDA shall implement corrective action, at no charge to the FCC or the industry, to correct any identified performance problems. The RNDA shall develop a Program Improvement Plan (PIP) that addresses each area identified during the annual performance review that requires performance improvement along with a time frame for completion. The PIP shall be presented to the FCC and/or its designee for review and acceptance prior to implementation. The annual assessment process shall not preclude Clients and general users from identifying performance problems to the RNDA and the FCC and/or its designee, as they occur, and from seeking resolution of such performance problems in an expeditious manner.

6.1.4 Self-Assessment and Reporting

The RNDA shall provide a self-assessment of its performance and action plan to correct any identified performance problems. Unless otherwise determined by the FCC and/or its designee, quarterly reports shall be delivered to the FCC and/or its designee within 30 days of the measurement period. The RNDA shall provide the following information:

- Summary of areas in which RNDA experienced difficulty and how the RNDA corrected the problem (RNDA internal and external difficulties included)
- Summary and description of incidences of Service Provider/Service Provider Agent, TFNA and User/User Agent dissatisfaction, and a description of the action taken by the RNDA to ensure the problem shall not reoccur
- Summary and total of written and oral complaints identified by performance metric
- Summary of major issues addressed by the RNDA including an evaluation of how the RNDA's activities influenced the outcome and how the outcome affected users

6.2 Performance Measurements

There are several ways that performance will be measured. Each derives input from different sources and, therefore, no single item should be considered of greater or lesser value than the others.

6.2.1 Assessment Period

On at least an annual basis, the FCC or its designee shall formally assess the performance of the RND and RNDA.

6.2.2 Corrective Action

The RNDA shall be required to implement an action plan to correct any identified performance problems within 30 calendar days.

6.2.3 Quality Assurance (QA)

The contractor's Quality Assurance Plan (QA Plan), required following contract award, shall follow the format, where applicable, of *IEEE Standard for Software Quality Assurance Processes* (Reference 10).

Upon establishment of the RND, the performance monitoring process shall include, but not be limited to, internal documented performance monitoring mechanisms to be developed and implemented by the RNDA and made available to the industry through the FCC and/or its designee

The RNDA shall have its representative(s) participate in calls as determined by the FCC and/or its designee. A formal agenda will be developed and agreed to by the RNDA and the FCC and/or its designee. The primary agenda items will include, at a minimum, the review of: (1) performance monitoring metrics and measurements; (2) complaints; (3) new developments (4) FCC and/or its designee reports; and (5) corrective action plans to resolve deficiencies in performance and/or complaints.

6.3 Performance Metrics

At a minimum, the following metrics shall be monitored by the RNDA so that the FCC and/or its designee can ensure performance of the requirements of the RND. The RNDA shall also produce performance reports (See Section 4).

6.3.1 Trouble Tickets/Outages

At a minimum, the RNDA shall track and report on the following trouble ticket and/or outage metrics:

- Number opened during the reporting period
- Number closed during the reporting period
- Number opened for over 30 calendar days.
- Number related to
  - System performance
  - Web site
  - Contractor ISP
  - Other
- Total quantity of trouble tickets opened and closed by month for a calendar year, with both the actual open and closed date for each ticket and the average open duration for all tickets.
- Quantity of System Outages Notifications to all RND Clients

6.3.2 Change Orders

At a minimum the RNDA shall track and report on the following metrics:

- List of change orders submitted to include:
  - Brief description of each change order
  - Type of change order
  - Date submitted
  - Status of each change order (*e.g.,* awaiting approval, approved but awaiting implementation, approved and implemented, denied)
  - Date approved or denied (if applicable)
  - The Written Notice of Changes Summarizing Potential Impact upon Service and Cost to be sent to the Contracting Officer's Representative (COR)

6.3.3 Communications

At a minimum, the RNDA shall track and report on the following metrics:

- Phone Calls
  - Received
  - Not Returned by Next Business Day
- Emailed Questions
  - Received
  - Not Responded to by Next Business Day
- General inquiries or questions received outside the normal business hours
  - Not Returned by Next Business Day

Section 7: Contract Data Requirements List (CDRL)

All items on this Contract Data Requirements List (CDRL) shall be approved by the FCC.

7.1 Ad Hoc Reports

Upon request by the FCC or its designee, the RNDA shall provide ad hoc reports concerning information contained in the RND system and performance of the system and its administrator.

7.2 Change Management Plan

The contractor shall provide a Change Management Plan to the FCC's Contracting Officer's Representative (COR) within 90 days of contract award. The COR shall review the Change Management Plan and request any necessary changes within 60 days, which the RNDA will effectuate before implementation.

7.3 Contract Change Management Plan

The contractor shall provide a Contract Change Management Plan within 90 days after the start of the first Option Year. The Contract Change Management Plan shall be reviewed and updated annually 60 days prior to the beginning of each Option Year.

7.4 Disaster/Continuity of Operations Plan

The contractor shall provide a Disaster/Continuity of Operations Plan within 60 days of contract award. The Disaster/Continuity of Operations Plan shall be updated annually 30 days prior to the beginning of each Option Year.

7.5 Implementation Plan

The contractor shall provide an Implementation Plan within 30 calendar days of contract award.

7.6 Management Reporting Plan

The contractor shall provide a Management Reporting Plan within 60 calendar days of contract award.

7.7 RND Administration System (RND System) Transition Plan

The contractor shall provide the RND System Transition Plan, which includes a list of items that are subject to transfer at the end of its term at the time of the new or modified system's acceptance. The Transition Plan shall be updated annually.

7.8 Program Improvement Plan (PIP)

The contractor shall provide a Program Improvement Plan (PIP) upon request by the FCC and/or its designee. The Contractor shall implement a continuous improvement program to identify and implement improvements to the services, processes, or system. Improvements shall include modifications that improve the end-user experience, result in lower costs, or that result in increased operational efficiency.

7.9 Quality Assurance (QA) Plan

The contractor shall furnish a Quality Assurance (QA) Plan within 120 calendar days of contract award.

7.10 Security Plan

The contractor shall provide a Security Plan within 45 calendar days of contract award. The Security Plan shall be updated annually 45 calendar days prior to the beginning of each Option Year.

7.11 Staffing Report

The contractor shall provide an initial staff report at the start of the contract and a monthly report, thereafter, to the FCC on staffing.

7.12 System Acceptance Plan

The contractor shall furnish a System Acceptance Plan within 30 calendar days of contract award.

7.13 System Implementation Plan

The contractor shall furnish a System Implementation Plan within 90 calendar days of contract award.

7.14 System Documentation Plan

The contractor shall provide a System Documentation Plan within 90 calendar days of contract award, the updated System Documentation Plan at the time of the new or modified system's acceptance, and thereafter the System Documentation Plan shall be updated annually. The contractor shall, according to the System Documentation Plan, provide the FCC-designated Contracting Officer's Representative (COR), for approval, with copies of the:

- System Design documentation describing in sufficient detail to guide normal operations, the system's structure, modules, and interactions
- System Operations documentation describing how to load, operate, and maintain the system, including system and application software upgrades, application modifications and host ports
- System User documentation describing the system and its features from the User/User Agent, TFNA, FCC, and Service Provider/Service Provider Agent perspectives

This documentation should be consistent with *IEEE Standard for Information Technology – Systems Design -- Software Design Descriptions* (Reference 7), *ISO/IEC/IEEE Standard for Systems and Software Engineering - Software Life Cycle Processes* (Reference 8), and *ISO/IEC/IEEE Systems and software engineering -- Requirements for acquirers and suppliers of user documentation* (Reference 5), respectively.

Within 90 days of contract award, the contractor shall ensure that the contractor will be compliant with the System Implementation Plan and System Documentation Plan, and contractor duties enumerated herein, and other pertinent industry/regulatory documents.

7.15 System Maintenance Plan

The contractor shall provide a System Maintenance Plan within 150 calendar days of contract award prior to new or modified system acceptance. The System Maintenance Plan shall be reviewed and updated annually 120 days prior to the beginning of each Option Year.

7.16 System Source Code

The contractor shall provide the System Source Code, and any other code or documentation, in machine-readable form, 180 days prior to contract termination.

7.17 System Test Plan

The contractor shall provide a System Test Plan within 30 days of contract award and shall be successfully completed within 90 calendar days of the contract award. This will include but not be limited to data upload, queries, running reports, and challenging security features. Confirm environment testing will simulate the production environment. The contractor will identify releases (i.e., alpha, beta, etc.) that reflect changes made to correct defects and in response to feedback from testers. This plan will be sufficient to identify all significant defects and delivery of an implementation plan.

7.18 Training Plan

The contractor shall provide a Training Plan for the training of the RNDA personnel pursuant to this TRD within 105 days of contract award. The Training Plan shall be reviewed and updated annually 30 days prior to the beginning of each Option Year.

7.19 Transition Plan

The contractor shall provide a Transition Plan 180 days prior to contract termination. The Transition Plan shall be a 90-day plan. However, the FCC may allow a possible 90-day extension depending on the need at the time of transition.

7.20 TRD Maintenance

The RNDA shall keep this Technical Requirements Document (TRD) current semi-annually, which would include change orders that have been implemented. Updated documents shall be provided to the FCC and/or its designee.

Section 8: RNDA Responsibilities for Processing Service Provider and TFNA Disconnected Numbers Reports

8.1 Service Provider and TFNA Disconnected Numbers Reports

The Service Provider Disconnected Numbers Report is filed monthly by Service Providers/Service Provider Agents in accordance with FCC Order 18-177 (Reference 9) and applicable industry guidelines. Each Service Provider that is assigned and/or ports in US geographic numbering resources shall complete the Service Provider Disconnected Numbers Report and submit it to the RNDA on the 15th of each month no later than11:59 pm. In the event that the 15th falls on a weekend or an RNDA-recognized holiday, Service Providers/Service Provider Agents shall complete the Service Provider Disconnected Numbers Report and submit it on the following business day.

The TFNA Disconnected Numbers Report is filed monthly by the TFNA in accordance with FCC Order 18-177 (Reference 9) and the TFNA's tariff on file with the FCC (Reference 13). The TFNA shall complete the TFNA Disconnected Numbers Report and submit it to the RNDA on the 15th of each month. In the event that the 15th falls on a weekend or an RNDA-recognized holiday, the TFNA shall complete the TFNA Disconnected Numbers Report and submit it on the following business day.

8.2 RNDA Responsibilities

The following sub-sections of the functional areas that fall within the RNDA's data collection, processing and disconnected numbers reporting responsibilities:

8.2.1 Point of Contact

The RNDA shall be the point of contact and shall assist Service Providers/Service Provider Agents and the TFNA in completing the appropriate disconnected numbers reports by clarifying the Service Provider and TFNA requirements to report and understand the disconnected numbers reporting process.

8.2.2 Contact List Maintenance

The RNDA shall periodically remind reporting entities in writing (via email) of the need to keep the list of contacts current and accurate.

8.2.3 Disconnected Numbers Data Requests

The RNDA shall send a monthly reminder to registered Service Provider/Service Provider Agent and TFNA system users to submit the monthly disconnected numbers reports.

8.2.4 Disconnected Numbers Reports Data Compilation and Processing

The RND system shall be capable of processing all of the data from the monthly Disconnected Numbers Reports and the Disconnected Toll Free Numbers Report as soon as possible but not later than the second business day following the submission of the reports.

8.2.5 Service Provider and TFNA User Support

The RNDA shall be available to the Service Provider/Service Provider Agent and TFNA system users to answer questions pertaining to any aspect of the disconnected numbers reporting process (*e.g.*, forms, instructions, processing, data assumptions, etc.). The RNDA shall also distribute periodic tips to registered Service Providers, Service Provider Agents and the TFNA, to assist them in avoiding common errors.

Section 9: Data Retention

9.1 Data Retention- General

The RNDA must establish and implement data retention policies and processes that support legal discovery, regulatory minimums pursuant to regulatory and statutory requirements consistent with the requirements in the documents identified in Section 10. The retention period may be subject to change pursuant to regulation or statute.

The RNDA shall take sufficient steps including backups to protect the retained records (See Section 3.15).

9.2 Retention of Records Relevant to User/User Agent Queries and Inquiries

In order to balance the Users'/User Agents' need to access data for legal purposes with the burdens and related costs of data retention, the RNDA shall retain for at least four years,[26] records relevant to Users/User Agents queries and inquiries. Records retained include Users/User Agents account metadata, Users/User Agents access (including time stamp), RND Query Request dates, associated number of TNs queried, and number of "yes", "no", and "no data" RND Query Responses. Records must be made accessible electronically to Users/User Agents upon request for the retention period (*e.g.*, via a request submitted in the User-facing interface).

9.3 Retention of Records Relevant to Service Provider/Service Provider Agent and TFNA Data Submissions

The RNDA shall retain for two years, records relevant to Service Provider/Service Provider Agent and TFNA disconnected number data report submissions. Records to be retained include system user access and system receipt of submission for each data report submission.

[26] Federal courts generally apply the 4-year federal "catch-all" limitations period from 28 U.S.C. § 1658(a) to claims brought under the TCPA. *See McCabe v. Lifetime Ent. Servs., LLC*, -- F. App'x --, 2019 WL 409440, at *1 (2d Cir. 2019); *Weitzner v. Sanofi Pasteur Inc.*, 909 F.3d 604, 608 (3d Cir. 2018); *Solis v. CitiMortgage, Inc.*, 700 F. App'x 965, 970 (11th Cir. 2017); *Coniglio v. Bank of Am., NA*, 638 F. App'x 972, 974 n.1 (11th Cir. 2016); *Sawyer v. Atlas Heating and Sheet Metal Works, Inc.*, 642 F.3d 560, 561 (7th Cir. 2011).

Records must be made accessible electronically to Service Providers/Service Provider Agents and the TFNA upon request for the retention period (*e.g.,* via a request submitted in the Service Provider-facing or TFNA-facing interface).

Section 10: List of References

1. Federal Communications Commission: *FCC Cyber Security Program,* FCCINST 1479.4 Effective Date, May 2011.

2. IEEE-SA Standards Board: *ISO/IECIEEE International Standard - Software and Systems engineering –Software testing – Part 3: Test documentation, Std 29119-3-2013*. See http://standards.ieee.org/findstds/standard/29119-3-2013.html.

3. National Fire Protection Association: *NFPA 1600® Standard on Continuity, Emergency, and Crisis Management, 2019 Ed.* Available at http://www.nfpa.org/.

4. Space and Naval Warfare Systems Command (SPAWAR): *Software Transition Plan (STrP), DI-IPSC-81429, Revision A,* January 10, 2000 validated July 8, 2013. Available at https://global.ihs.com/doc_detail.cfm?&item_s_key=00227803&item_key_date=860523&input_doc_number=DI%2DIPSC%2D81429&input_doc_title=.

5. IEEE-SA Standards Board: ISO/IEC*IEEE Systems and software engineering – Requirements for acquirers and suppliers of user documentation, Std 26512-2011.* Available at https://standards.ieee.org/standard/26512-2011.html

6. National Institute of Standards and Technology (NIST): *Guide for Developing Security Plans for Federal Information Systems, NIST Special Publication 800-18 Revision 1*. February 2006. Available at http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-18r1.pdf.

7. IEEE-SA Standards Board: *IEEE Standard for Information Technology – Systems Design -- Software Design Descriptions*, Std 1016-2009. July 20, 2009. Available at https://standards.ieee.org/standard/1016-2009.html.

8. IEEE SA Standards Board: *ISO/IEC/IEEE Standard for Systems and Software Engineering - Software Life Cycle Processes, Std 12207-2017. November 1, 2017*. Available at http://standards.ieee.org/findstds/standard/12207-2017.html.

9. Federal Communications Commission: *In the Matter of Advanced Methods to Target and Eliminate Unlawful Robocalls, Second Report and Order* in CG Docket No. 17-59, FCC 18-177 (adopted December 12, 2018). Available at: https://docs.fcc.gov/public/attachments/FCC-18-177A1.pdf.

10. IEEE-SA Standards Board: *IEEE Standard for Software Quality Assurance Processes*, IEEE Std 730-2014. Available at: http://standards.ieee.org/findstds/standard/730-2014.html.

11. Code of Federal Regulations (CFR), Title 47, Volume 3, Parts 40-69, Telecommunications. Available at: https://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&tpl=/ecfrbrowse/Title47/47cfrv3_02.tpl.

12. Department of Defense (DoD), US General Services Administration (GSA) and the National Aeronautics and Space Administration (NASA): *Federal Acquisition Regulation (FAR).* Available at: https://www.acquisition.gov/browse/index/far.

13. Somos, Inc.: *800 Service Management System (SMS/800) Toll-Free Number Registry (TFN Registry) Functions*, TARIFF F.C.C. NO. 1, February 2018. Available at: https://s3.amazonaws.com/files-prod.somos.com/documents/SMS800FunctionsTariff.pdf

14. National Institute of Standards and Technology (NIST): *Digital Identity Guidelines*, SP 800-63, June 2017. Available at: https://pages.nist.gov/800-63-3/.

Standards documents identified above to which the RNDA is held to comply under this contract shall be deemed to be the latest version of those documents. However, the RNDA is obliged to comply with updated standards only where consistent with FCC regulations and direction.

Appendix A: Abbreviations

API	Application Programing Interface
ATIS	Alliance for Telecommunications Industry Solutions
CDRL	Contract Data Requirements List
CFR	Code of Federal Regulations
COR	Contracting Officer's Representative
EFT	Electronic File Transfer
FACA	Federal Advisory Committee Act
FAQ	Frequently Asked Question
FCC	Federal Communications Commission
GUI	Graphical User Interface
IETF	Internet Engineering Task Force
INC	ATIS Industry Numbering Committee
ITU	International Telecommunications Union
LNP	Local Number Portability
NANP	North American Numbering Plan
NANPA	North American Numbering Plan Administrator
NIST	National Institute of Standards and Technology
NPA	Numbering Plan Area (*i.e.,* area code)
NXX	3-Digit Central Office Code
PIP	Program Improvement Plan
QA	Quality Assurance
RespOrg	Responsible Organization
RFP	Request for Proposal
RND	Reassigned Number Database
RNDA	Reassigned Number Database Administrator
sFTP	Secure File Transfer Protocol
SMS	Service Management System
SPOC	Single Point of Contact
STrP	Software Transition Plan
TFNA	Toll Free Number Administrator
TN(s)	Telephone Number(s)
VoIP	Voice Over Internet Protocol

Appendix B: Terms & Definitions

Audit Files	The ability for Service Providers/Service Provider Agents and Toll Free Number Administrator to obtain information about their records submitted to the RND.
Auditor	The appropriate bureau(s) within the FCC or other appropriate governmental entity, or other neutral vendor selected to audit the administration functions of the RND.
Billing and Collection Agent	The entity responsible for the collection of funds to support numbering administration for telecommunications services from the United States telecommunications industry and NANP member countries (47 CFR §52.7 (f); see also 47 CFR §52.16).
Client	Any entity that has registered system user access to the Reassigned Number Database. This could be a Service Provider, Service Provider Agent, User, User Agent, Toll Free Number Administrator or the FCC and/or its designee.
Client Activity	Any interactions between the RNDA and a Client.
Company Identifier	A unique identifying code, based upon the profile type, that is assigned to each Service Provider, Service Provider Agent, User, User Agent, Toll Free Number Administrator and the FCC.
Contractor	The vendor contracted by the FCC to be the RNDA
Date of Prior Express Consent	The date of which a customer provided consent or has otherwise been provided authorization for a calling entity to contact them at a specific telephone number (See also CFR 64.1200(m)).
Disconnect Date	The date in which a telephone number is permanently disconnected by a Service Provider/TFNA. This date will be uploaded into the RND by the Service Provider/Service Provider Agent/ Toll Free Number Administrator.
Emergency Updates	The ability for the RNDA to make updates on behalf of the Service Provider/Service Provider Agent/Toll Free Number Administrator in the case of incorrect information that was submitted/uploaded into the RND.
Federal Risk and Authorization Management Program (FedRAMP)	A government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.
Industry Numbering Committee (INC)	An industry forum operating under the auspices of the ATIS. Its mission is to provide an open forum to address and resolve industry-wide issues associated with the planning, administration, allocation, assignment and use of numbering resources and related dialing considerations for public telecommunications within the NANP area.
Logon Credentials	User ID and Password that provides access to the RND pursuant to the RND access requirements.
Modify Date	The date on which a record was modified within the RND.

North American Numbering Council (NANC)	A Federal Advisory Committee established pursuant to the United States Federal Advisory Committee Act (FACA) as amended, 5 U.S.C. App 2. The purpose of the NANC is to advise the FCC and to make recommendations that foster efficient and impartial NANP administration. The NANC advises the FCC on numbering policy and technical issues in areas of responsibility the FCC has entrusted to the NANC, with a focus on examining numbering in the changing, modern world of communications.
North American Numbering Plan (NANP)	The basic numbering scheme for the public switched telecommunications networks in the following 20 countries (formerly known as World Zone 1): Anguilla, Antigua & Barbuda, Bahamas, Barbados, Bermuda, British Virgin Islands, Canada, Cayman Islands, Dominica, Dominican Republic, Grenada, Jamaica, Montserrat, Sint Maarten, St. Kitts & Nevis, St. Lucia, St. Vincent & the Grenadines, Trinidad & Tobago, Turks & Caicos Islands, and the United States and its territories (including Puerto Rico, the US Virgin Islands, Guam, the Commonwealth of the Northern Mariana Islands, and American Samoa). The format of the NANP is in compliance with ITU standards as detailed in Recommendation E.164. See 47 CFR §52.5 (d).
NPA	A unique three-digit number that identifies the telephone service region.
NXX	A central office code (*i.e.*, the sub-NPA codes in a telephone number, digits D-E-F of a 10-digit number); often referred to as "NXX codes" because they are in the format of "NXX", where N is a number from 2 to 9 and X is a number from 0 to 9.
Offeror	The company submitting a proposal response to an RFP.
Program Improvement Plan	A program improvement plan is a formal document stating any recurring performance issues along with goals that are needed to achieve in order to regain good standing (usually with a specific timeline to complete the plan).
Permanent Disconnection	Occurs when a subscriber permanently has relinquished a number, or the provider permanently has reversed its assignment of the number to the subscriber such that the number has been disassociated with the subscriber for active service in the service provider's or Toll Free Administrator's records. Permanently disconnected numbers therefore do not include instances where the phone number is still associated with the subscriber, such as when a subscriber's phone service has been disconnected temporarily for nonpayment of a bill or when a consumer ports a number to another provider. A ported number remains assigned to and associated with the same consumer even though a different provider serves the consumer after the number is ported. (see also 47 CFR 52.103(d) and 47 CFR 64.1200 (l)(3))
Service Provider's/Service Provider Agent's/Toll Free Administrator's Query	The Service Provider's/Service Provider Agent's/Toll Free Administrator's ability to request and retrieve data stored in the RND.

Query Originator	User, User Agent, or FCC that submits an RND Query Request
Reassigned Number Database	The database which will contain a list of all US geographic and Toll Free NANP numbers that have been permanently disconnected and the disconnect date that Users and User Agents will be able to query to validate whether a telephone number has the potential to have been reassigned.
Reassigned Number Database Administrator	The entity which will maintain the Reassigned Number Database.
RESTful API	An application programing interface (API) that uses HTTP requests to GET, PUT, POST and DELETE data.
RND Query Request	A request of the RND in the form of a ten-digit TN and the Date of Prior Express Consent submitted by the User/User Agent.
RND Query Response	A response from the RND to the User/User Agent in the format of "Yes", "No", or "No Data"
Service Provider	Any telecommunications carrier or other entity that receives numbering resources from the NANPA, a Pooling Administrator or a telecommunications carrier for the purpose of providing or establishing telecommunications service. For the purposes of this part, the term "service provider" includes an interconnected VoIP service provider. (47 CFR §52.5 (e)).
Service Provider Agent	Any party authorized to act on behalf of a Service Provider for the purposes of fulfilling the requirements of the service provider to provide permanently disconnected number information to the RND.
Service Provider Disconnected Numbers Report	A report filed monthly by each Service Provider (or its Service Provider Agent) with the RNDA that identifies each US geographic telephone number allocated to or ported-in to the Service Provider that has been permanently disconnected since the last report was filed. The report contains the US geographic telephone number and the date it was permanently disconnected.
Subcontractor	An organization providing services to the Contractor. One not in the employment of the contractor, who is performing designated services and functions contained within this document.
System Acceptance Plan	A plan developed by the contractor that is consistent where applicable with *ISO/IEC/IEEE International Standard - Software and Systems engineering –Software testing – Part 3: Test documentation*.
System Documentation Plan	The plan used to schedule and allocate resources to create and maintain technical content deliverables for a specified project or product. The plan describes the audiences, content types and output media, and provides a schedule for development and completion of deliverables.
System Implementation Plan	The carrying out, execution, or practice of a plan, a method, or any design, idea, model, specification, standard or policy for doing something. As such, implementation is the action that must follow any preliminary thinking in order for something to actually happen.

System Source Code	In computing, source code is any collection of code, possibly with comments, written using a human-readable programming language, usually as plain text. The source code is often transformed by an assembler or compiler into binary machine code understood by the computer.
Telephone Number(s)	A number assigned to a telephone line for a specific phone or set of phones that is used to call that phone.
Term of Administration	The contractor's contract shall be for a term determined by the FCC; It shall be the period of time for which these requirements shall apply. At any time prior to the termination of the initial or subsequent Term of Administration, the Term of Administration may be renewed with the approval of the RND contractor and the appropriate regulatory authorities.
Toll Free Number Administrator (TFNA)	The entity which allocates toll free numbers to RespOrgs and maintains the SMS database which contains all toll free telephone numbers.
Toll Free Number Administrator (TFNA) Disconnected Numbers Report	A report filed monthly by the Toll Free Number Administrator with the RNDA that identifies each toll free telephone number that has been permanently disconnected since the last report was filed. The report contains the toll free telephone number and the date it was permanently disconnected.
Training Plan	A training plan is a detailed document that guides the planning and delivery of RNDA personnel instruction.
Transition Plan	A formal business transition plan puts the goals, priorities and strategies in place for a successful transition.
User	Any person or entity that queries the Reassigned Number Database to determine whether a telephone number has the potential to have been reassigned.
User Agent	Any authorized person or entity acting on behalf of another User that queries the Reassigned Number Database to determine whether a telephone number has the potential to have been reassigned.
User/User Agent RND Query Request Transaction Log	A transaction log of the User/User Agent queries into the RND.
User ID(s)	A unique identification code that is assigned to every individual with log-in access the RND.