



HARRIS, WILTSHIRE & GRANNIS LLP

EX PARTE OR LATE FILED

REDACTED—FOR PUBLIC INSPECTION

September 24, 2014

Ms. Marlene H. Dortch
Secretary
Federal Communications Commission
445 12th Street, S.W.
Washington, DC 20554

ACCEPTED/FILED

SEP 24 2014

Federal Communications Commission
Office of the Secretary

Mr. Sanford Williams
Competition Policy Division
Wireline Competition Bureau
Federal Communications Commission
445 12th Street, SW, Room 5-C217
Washington, DC 20554

DOCKET FILE COPY ORIGINAL

Re: *Telephone Number Portability, et al.*, CC Docket No. 95-116, WC Docket No. 09-109

Dear Ms. Dortch and Mr. Williams:

Enclosed is an Ex Parte letter of Telcordia Technologies, Inc., d/b/a iconectiv in response to Nuestar's Reply Comments.¹

As required by paragraph 15 of the *Revised Protective Order*,² we submit: (a) one copy of this Ex Parte letter containing Confidential and Highly Confidential Information to the Secretary's Office along with this cover letter, (b) two copies of this Ex Parte letter in redacted form to the Secretary's Office along with a cover letter; and (c) two copies of this Ex Parte letter containing Confidential and Highly Confidential Information to Sanford Williams along with this cover letter. We will also file a copy of the redacted version via ECFS.

¹ Reply Comments of Neustar, Inc., WC Docket No. 09-109 and CC Docket No. 95-116 (filed August 22, 2014).

² *Petition of Telcordia Technologies, Inc. to Reform or Strike Amendment 70, to Institute Competitive Bidding for Number Portability Administration and to End the NAPM LLC's Interim Role in Number Portability Administration Contract, Telephone Number Portability*, WC Docket No. 09-109, CC Docket No. 95-116, Revised Protective Order, DA 14-881, (Wireline Comp. Bur. rel. June 25, 2014).

No. of Copies rec'd 0+1
List ABCDE

Ms. Marlene H. Dortch
Mr. Sanford Williams
September 24, 2014
Page 2 of 2

Sincerely,

A handwritten signature in black ink, appearing to read "John T. Nakahata". The signature is fluid and cursive, with a long horizontal stroke at the end.

John T. Nakahata
*Counsel for Telcordia Technologies,
Inc., d/b/a/ iconectiv*

REDACTED—FOR PUBLIC INSPECTION

ACCEPTED/FILED

SEP 24 2014

Federal Communications Commission
Office of the Secretary

BEFORE THE
FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON, D.C. 20554

In the Matter of:

Petition of Telcordia Technologies, Inc.
To Reform or Strike Amendment 70, To
Institute a Competitive Bidding for
Number Portability Administration, and
To End the LLC's Interim Role in
Number Portability Administration
Contract Management

Telephone Number Portability

WC Docket No. 09-109

WC Docket No. 07-149

CC Docket No. 95-116

**EX PARTE RESPONSE OF TELCORDIA TECHNOLOGIES, INC., D/B/A
ICONECTIV TO NEUSTAR REPLY COMMENTS**

Jason A. Carey
Erin B. Sheppard
MCKENNA LONG & ALDRIDGE LLP
1900 K St., N.W.
Washington, D.C. 20006

James Arden Barnett, Jr.
Rear Admiral USN (Ret.)
VENABLE LLP
575 Seventh Street, N.W.
Washington, DC 20004

John T. Nakahata
Christopher J. Wright
Amy E. Richardson
Mark D. Davis
Randall W. Sifers
Kristine Devine
Stephen Miller
Anne K. Langer
John R. Grimm

HARRIS, WILTSHIRE & GRANNIS LLP
1919 M Street NW, Eighth Floor
Washington, D.C. 20036
(202) 730-1320
jnakahata@hwglaw.com

September 24, 2014

TABLE OF CONTENTS

EXECUTIVE SUMMARY 1

ARGUMENT..... 4

I. The RFP Contains Robust Security Requirements and the Concerns Neustar Highlights Are Logically Encompassed Within Those Existing Requirements..... 4

A. The Existing RFP Addresses Each of the Requirements Highlighted In Neustar’s Reply Comments 4

B. Telcordia’s Proposal Amply Demonstrates Its Ability and Willingness to Satisfy Law Enforcement Agencies’ Security Needs 12

C. ****BEGIN HIGHLY CONFIDENTIAL**** [REDACTED] ****END**
[REDACTED] **HIGHLY CONFIDENTIAL**** 13

II. Even if it Applied, Federal Procurement Law Would Not Require That the Competition Be Reopened..... 14

III. Telcordia’s Ability to Satisfy Specified Security Criteria — Such as Possession of a Security Clearance — Concerns a Matter of Responsibility For Which Federal Procurement Law Permits Post-Selection Communications..... 19

IV. Neustar’s Argument that the SWG and NANC Reports Violate the FACA Ignores the Law and is Wrong on the Merits 20

A. FACA’s Fairly Balanced Requirement Does Not Apply to the SWG, and Even If It Did, the NANC and SWG Were Fairly Balanced..... 20

B. Even if the Fairly Balanced Requirement Applied, that Would Not Be a Reason for the Commission to Disregard the NANC’s Recommendation..... 23

CONCLUSION 26

REDACTED—FOR PUBLIC INSPECTION

EXECUTIVE SUMMARY

The purpose of a solicitation is not to detail the minutia of what will need to be accomplished during performance of a contract. Rather, it is to identify the buyer's requirements, at a reasonable level of specificity, so that (1) the offerors can describe their approach to fulfilling those requirements, and (2) the buyer can intelligently evaluate each offeror's ability to meet its needs. That is exactly what the solicitation did here. It identified NAPM's requirements for security and the Enhanced Law Enforcement Platform ("ELEP"), and provided the Future of the Number Portability Administration Center ("FoNPAC"), the North American Portability Management LLC ("NAPM"), the North American Numbering Council ("NANC") and the NANC's Selection Working Group ("SWG") with a basis on which to assess whether the offerors could successfully meet the security and ELEP requirements of the LNPA contract.

Neustar would hold this non-federal procurement — and, by implication, every federal procurement — to an unnecessary (and unattainable) standard. It would require solicitations, not just to set forth the buyer's fundamental requirements, but to forecast with precision exactly how the awardee will fulfill those requirements during performance. There is no basis for such an extraordinary and extreme position. Here, the RFP established robust security and ELEP requirements; Telcordia fully addressed and satisfied those requirements; and the details of implementation will obviously be addressed as a matter of routine contract administration.

REDACTED—FOR PUBLIC INSPECTION

In a desperate attempt to scare the Commission, and wheedle its way back into a competition it already lost fair-and-square, Neustar asserts that the solicitation did not address certain security and ELEP matters. That assertion, however, ignores the plain language and sweeping requirements of the solicitation. In reality, the solicitation's security and ELEP requirements logically encompass all of the areas that Neustar complains about. The level of detail that Neustar now demands was neither necessary nor required at the proposal stage. The details have not been omitted; they are simply matters of technical implementation properly left for contract administration and contract performance. The solicitation more than adequately described the relevant security and ELEP requirements.

In its vain attempt to pry its way back into the competition, Neustar also relies upon inapplicable and squarely distinguishable federal procurement principles and decisions. All of Neustar's cited cases involve situations where a federal agency either (1) relaxed a material solicitation requirement, or (2) allowed an offeror whose proposal did not meet a stated solicitation requirement to fix its proposal in order to make it acceptable. Neither situation exists here. NAPM and the Commission are not relaxing, and will not relax, any requirements of the solicitation. Rather, they will work with Telcordia as the awardee to develop a detailed plan to implement those requirements, fully and effectively, during performance. And NAPM and the Commission are not allowing Telcordia to fix a non-compliant proposal. To the contrary, Telcordia's

REDACTED—FOR PUBLIC INSPECTION

proposal provided a compliant and vigorous solution for meeting — and exceeding — the solicitation’s security and ELEP requirements.

The solicitation provides a robust framework for assessing each offeror’s security and ELEP capabilities. Telcordia is ready and willing to engage with NAPM and the Commission to ensure that those requirements are fully built out and implemented during contract performance. None of the authorities Neustar relies upon in its Reply Comments or Supplemental Comments preclude such a dialogue or require further competition. The Commission should expeditiously proceed with recommending award to Telcordia and permit Telcordia to enter into contract negotiations with NAPM to that end.

Finally, Neustar’s argument — made for the first time in its Reply — that the Commission cannot rely on NANC’s recommendation because the Selection Working Group did not comply with the Federal Advisory Committee Act (“FACA”) is also meritless. Under General Services Administration rules implementing the FACA, the SWG is not required to meet FACA requirements because NANC conducted its own subsequent review and evaluation. In any event, even if NANC and SWG violated the FACA, by seeking public comment, the Commission has provided all the remedy that would be required. This is just another of Neustar’s spurious arguments designed to manufacture delay.

ARGUMENT

I. The RFP Contains Robust Security Requirements and the Concerns Neustar Highlights Are Logically Encompassed Within Those Existing Requirements

The RFP, its Technical Requirements Document (“TRD”), and the Functional Requirements Specification (“FRS”) together outline robust security requirements. Telcordia viewed these documents as establishing a robust set of security requirements and interpreted each of those requirements to apply equally to both the ELEP and NPAC SMS. Moreover, each of the areas Neustar claims are “omitted” are logically subsumed in these existing RFP requirements. And Telcordia’s proposal clearly and directly addressed its compliance with each of those requirements — with the same level of detail Neustar provided in its own proposal.

A. The Existing RFP Addresses Each of the Requirements Highlighted In Neustar’s Reply Comments

The RFP, Technical Requirements Document (“TRD”), and Functional Requirements Specification (“FRS”) (collectively the “solicitation documents”), outline detailed security requirements applicable to both the NPAC SMS and ELEP. Telcordia applied the security requirements in the RFP and the FRS — including authentication, access control, non-repudiation, and availability — to both the ELEP and the NPAC SMS. Telcordia also anticipated providing any additional functionality required for the ELEP in response to direct needs voiced by the law enforcement community during the course of implementation.

REDACTED—FOR PUBLIC INSPECTION

Section 7 of the FRS in particular outlines a number of fundamental security and interface design requirements that plainly encompass the security areas Neustar now claims are not covered by the RFP. And those requirements apply equally to both the NPAC SMS and the ELEP system. Specifically, Telcordia viewed the following FRS sections to be directly applicable to the Enhanced Law Enforcement Platform:

- Section 7.2, “Identification” — describes that each user is uniquely identified as well as some requirements for User IDs.
- Section 7.3, “Authentication” — indicates that all users shall be authenticated and provides password requirements
- Section 7.4, “Access Control” — provides authorization requirements that indicates what data/functions users may access and also describes encryption mechanisms
- Section 7.5, “Data and System Integrity” — provides requirements to prevent/detect corruption of data and requests for data
- Section 7.6, “Audit” — describes detecting and reporting inappropriate access and providing logs to perform after the fact investigations
- Section 7.7, “Continuity of Service” — provides requirements for detecting system degradation and backup procedures
- Section 7.8, “Software Vendor” — provides requirements for having a corporate software development policy and prohibits “backdoors”.
- Section 7.9, “Mechanized Security Environment” — for machine-to-machine interfaces, describes authentication, detecting man-in-the-middle attacks, encryption, non-repudiation, and access control

REDACTED—FOR PUBLIC INSPECTION

****BEGIN HIGHLY CONFIDENTIAL**** [REDACTED]

[REDACTED] **** END HIGHLY CONFIDENTIAL****

In addition to the requirements in FRS Section 7, the vast majority of the security provisions that Neustar deems “essential” for limiting access to ELEP are also already incorporated in Section 11.2 of the RFP. That section highlights twenty-one different requirements applicable to the offerors’ ELEP solutions. Those requirements cover both security and key functional requirements. For example, RFP section 11.2, Requirement 7 provides: “The LNPA shall employ an LSMS to provision current and historical Enhanced Law Enforcement Platform Data Elements into the Enhanced Law Enforcement Platform.” Section 11.2 ensures that the LNPA will provide the law enforcement community with the required Data Elements within the same response time that the NPAC currently supports. And the FRS provides detailed requirements for downloading data to the LSMS.

Moreover, each item on the list of requirements Neustar characterizes as necessary to protect national security interests is already encompassed by the RFP and its incorporated documents.² Try as Neustar might to spark doubt within the Commission,

¹ See Telcordia Response to BAFO Survey Question 2.6 at 3 (Telcordia10008).

² Neustar Reply Comments at 65-66.

REDACTED—FOR PUBLIC INSPECTION

the existing LNPA solicitation documents, anticipated Master Agreement, and anticipated service agreements with law enforcement provide a sound framework for addressing each of the requirements Neustar erroneously claims are “omitted” from the RFP and associated documents.

The following chart lists each of Neustar’s purportedly additional requirements and lists the various existing solicitation provisions and incorporated documents that address those requirements.

Allegedly Omitted Requirement	Solicitation Requirement(s) that Encompasses the Requirement at Issue
Requiring that queries of the system remain confidential so that a potential criminal will not learn that law enforcement is investigating them	RFP § 11.2, Req. 8: “The LNPA shall provide access to the Enhanced Law Enforcement Platform by virtual private network (machine to machine) or Internet (person to GUI). Access to [ELEP] shall be accomplished by authenticated, secure and encrypted means.”
Requiring the LNPA vendor to supply, at a minimum, the same information that is currently provided, including current and historical information, in real or near real time immediately upon granting the contract	RFP § 11.2, Req. 6 (requiring the LNPA to make available specific ELEP Data Elements), Req. 7 (requiring the LNPA to “employ an LSMS to provision current and historical ELEP Data Elements”), and Req. 9 (limiting information provided to Qualified Recipients to Enhanced Law Enforcement Platform Data Elements)
Requiring the LNPA vendor to provide an API that permits a variety of platforms immediately to query large batches of numbers from multiple locations	RFP § 11.2, Req. 8 (provide machine to machine access) and Req. 10 (allowing Qualified Recipients to perform unlimited queries but limiting to no more than 100 TNs per query)

REDACTED—FOR PUBLIC INSPECTION

<p>Ensuring the LNPA vendor does not have unwarranted visibility into the queries submitted by a law enforcement agency in order to maintain the confidentiality and integrity of those investigations</p>	<p>RFP § 11.2, Req. 13 (requiring ELEP user data to remain confidential information); FRS § 7.4.1 (related to user access control and authentication)</p>
<p>Prohibiting remote write or administrator access outside of the United States or through a foreign corporate-parent entity</p>	<p>RFP § 6.4, Req. 1 (requiring at least two completely redundant NPAC/SMS data centers based geographically in the continental United States); RFP § 6.7, Req. 2 (requiring all data to be stored in the continental United States and mandating that “no data relating to the Service will be stored, maintained, or warehoused, in a physical or electronic form, at, in, or through a site, on services or otherwise, located outside of the continental United States.”); FRS § 7.4.2, Req. 7-55 (requiring that control of access to resources be based on authenticated user identification)</p>
<p>Prohibiting the LNPA vendor from tracking, logging, or preserving the queries submitted by law enforcement agencies</p>	<p>RFP § 11.2, Req. 2 (limiting access to Qualified Recipients) and Req. 5 (requiring execution of an agreement with ELEP users, which can provide additional specific details to be satisfied by the LNPA)</p>
<p>Requiring LNPA personnel with secure network access to be U.S. citizens capable of maintaining a security clearance</p>	<p>RFP § 11.2, Req. 5³ (requiring execution of an agreement with ELEP users, which can provide additional specific details to be satisfied by the</p>

³ The broad security requirements included in the RFP fairly encompass the specific concerns raised by Neustar. Detailed criteria for granting access to the NPAC SMS or the ELEP system were never intended to be spelled out in the solicitation. Rather, these detailed requirements can be addressed during contract negotiations and can then be included in the Master Agreements to be negotiated post award, as contemplated by Section 16.1 of the RFP. Both the Master Agreements and ELEP Service Agreements provide additional avenues for imposing any detailed criteria to flesh out existing requirements already addressed within the RFP’s overarching security framework.

REDACTED—FOR PUBLIC INSPECTION

	LNPA); FRS § 7.4.1 (establishing access control requirements)
Requiring the LNPA vendor, in coordination with law enforcement, to assess the suitability of individuals with access to the LNP system	RFP § 11.2, Req. 1, Req. 2, Req. 11, Req. 12, Req. 14, Req. 15, and Req. 16 (addressing a range of requirements such as establishment of user agreements, access limitations, restricting uses to lawful purposes, annual verification requirements); RFP § 5.1 (new user evaluation and related processes); FRS §§ 7.4.1-7.4.2 (establishing access control requirements)
Prioritizing repairs and restoration if the LEAP system fails in whole or in part	RFP § 6.4 (“NPAC/SMS Data Center Redundancy Requirements”); RFP § 9 (establishing various service level requirements; FRS § 7.7 (establishing continuity of service requirements)
Requiring a written security plan approved by NAPM LLC in consultation with federal law enforcement and other agencies, and filed with the Commission	RFP § 6.7, Req. 1 (maintain and enforce at all times adequate NPAC data center safety and physical security procedures); RFP § 4.4, Req. 3 (Annual audit will address NPAC and facilities security and overall compliance with industry standards for data center operations); RFP § 11.2, Req. 5 (requiring execution of an agreement with ELEP users, which can provide additional specific details to be satisfied by the LNPA) ⁴

⁴ It goes without saying that Telcordia’s efforts to address such security will need to be implemented in accordance with a written plan, making any specified need for such a written security plan in advance of such discussions unnecessary (*see, e.g.* Telcordia Response to BAFO Survey Question 2.6 at 8 (Telcordia10013) (discussing security audits that will require that a written security plan be in place)).

REDACTED—FOR PUBLIC INSPECTION

Requiring compliance and incident reports, as well as a process for regularly scheduled and random compliance inspections	RFP § 9 (Service level requirements, including system security and security error logs); RFP §§ 11.3 (LNPA Reports to NAPM)-11.4 (LNPA Reports to the FCC); FRS § 7.6.2 (Reporting and Intrusion Detection requirements)
Requiring authentication of law enforcement credentials for access to the system	RFP § 11.2, Req. 2, Req. 8, Req. 11, Req. 12 and Req. 14 (establishing a range of authentication, access control, and verification requirements)
Requiring the LNPA vendor to ensure continuity of operations of the system and establish at least one secure backup data center for that purpose	RFP § 6.4 (creating data center redundancy requirements); FRS § 7.7 (establishing continuity of service requirements)
Requiring audits of the system to detect access to law enforcement queries by employees or contractors of the LNPA vendor or any other third party	RFP § 9 (SLR 17, System Security, Security Error Log)
Requiring the LNPA to provide to the NAPM LLC and file with the Commission a detailed accounting of supply chain standards and procedures specific to the query system ⁵	FRS § 7.8 (Software Vendor Requirements)

In sum, the totality of the LNPA RFP security requirements — including RFP section 11.2, the Technical Requirements Document, and the FRS — present a comprehensive and robust framework under which the Commission and law enforcement

⁵ Telcordia will ensure that its approach to these requirements meets stakeholders' needs regarding supply chain standards. And, as Telcordia has repeatedly emphasized, it is using a greenfield approach for this contract, with entirely new code for the U.S. NPAC developed in the U.S. and used only in the U.S.

REDACTED—FOR PUBLIC INSPECTION

may work with the LNPA to address more granular requirements as part of contract administration. To that end, Telcordia's proposal addressed its willingness and eagerness to work in tandem with NPAC customers — to include law enforcement — to “engage on an ongoing basis with the Industry and the NAPM LLC to ensure the appropriate policies are implemented and maintained to protect the privacy and confidential information of NPAC customers and their respective subscribers, customers and end users as the Services continue to evolve.”⁶ ****BEGIN HIGHLY CONFIDENTIAL****

[REDACTED]

⁶ Telcordia Response to BAFO Survey Question 2.6 at 2.

⁷ *Id.* at 3 (Telcordia10008).

⁸ **** BEGIN HIGHLY CONFIDENTIAL **** [REDACTED]

[REDACTED]

****END HIGHLY CONFIDENTIAL****

⁹ See RFP § 11.2, Req. 5 (noting that access to ELEP would require each qualified agency to enter into a separate ELEP service agreement).

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] **END

HIGHLY CONFIDENTIAL**

* * *

Neustar's Reply Comments rely on sensationalized fear-mongering at the expense of reality. A fair reading of the solicitation documents confirms that the solicitation documents include a broad range of security requirements applicable to both ELEP and the NPAC SMS. Moreover, each of the laundry list of requirements Neustar highlights on pages 65 through 66 of its Reply Comments are logically encompassed by the existing security and other associated technical requirements contained at various places throughout the solicitation documents. There is no need to revise the solicitation, and no reason to give Neustar another unfair bite at the apple.

B. Telcordia's Proposal Amply Demonstrates Its Ability and Willingness to Satisfy Law Enforcement Agencies' Security Needs

BEGIN HIGHLY CONFIDENTIAL [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

REDACTED—FOR PUBLIC INSPECTION

[REDACTED]
[REDACTED]
[REDACTED] [REDACTED]
[REDACTED] ****END HIGHLY**

CONFIDENTIAL**

Critically, contrary to Neustar's allegations in its Supplemental Reply Comments, Telcordia's proposal does, in fact, address each of the technical aspects Neustar challenges in that filing. Telcordia refers the FCC to its detailed Supplemental Response filed separately with the FCC for a more detailed response to the specific allegations raised in Neustar's Supplemental Comments.

C. ****BEGIN HIGHLY CONFIDENTIAL**** [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

10 ****BEGIN HIGHLY CONFIDENTIAL**** [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED] ****END**
HIGHLY CONFIDENTIAL**

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] ****END HIGHLY CONFIDENTIAL****

II. Even if it Applied, Federal Procurement Law Would Not Require That the Competition Be Reopened

The federal procurement law and decisions that Neustar cites do not help its case. As an initial matter, Neustar concedes that this is not a federal procurement. Therefore, federal procurement principles do not apply to, or constrain, the Commission's decision regarding whether to follow the NANC's award recommendation and designate Telcordia as the LNPA. Instead, the Commission's LNPA selection simply must be reasonable and not arbitrary and capricious. As explained in detail above, the RFP wholly encompasses each of the security provisions Neustar claims have been omitted. Moreover, the solicitation affords the Commission — and Federal Law Enforcement Agencies — substantial flexibility to specify additional details during the course of negotiating both the Master Agreements and ELEP Service Agreements. As such, the Commission can reasonably conclude that the existing solicitation is more than sufficient to satisfy its needs and proceed with the recommended award to Telcordia on that basis.

On top of that, even if federal procurement rules did apply, they would not help Neustar here. Neustar cites one line of decisions where an agency either relaxed

REDACTED—FOR PUBLIC INSPECTION

mandatory solicitation requirements to permit an offeror's otherwise unacceptable proposal to remain eligible for award¹¹ or provided one offeror an opportunity to rectify a shortcoming of its own proposal in order to render its proposal acceptable and eligible for award.¹² Under both of these categories of cases, the problem was that the awardee failed to satisfy the solicitation's stated requirements, while all other offerors complied, resulting in an unfair competition.

¹¹ *Hunt Bldg. Co. v. United States*, 61 Fed. Cl. 243, 276 (2004) (relaxing the solicitation requirement that legal documents to be utilized after selection must remain "substantially identical" to forms included in the solicitation constituted an impermissible relaxation of the solicitation's requirements for the benefit of a single offeror); *Beta Analytics Int'l, Inv. v. United States*, 44 Fed. Cl. 131, 139 (1999) (awarding a contract to offeror with noncompliant proposal imposed a disadvantage on other offerors for simply following the solicitation's mandatory terms); *Mangi Environmental Group, Inc. v. United States*, 47 Fed. Cl. 10, 17-18 (2000) (waiving material defect in awardee's proposal prejudicial because awardee should have been found unacceptable and ineligible for award).

¹² *See The Analysis Group, LLC*, B-401726, B-401726.2, 2009 CPD ¶ 237 (Comp. Gen. Nov. 13, 2006) (agency's permitting an offeror to remove indemnification provision that rendered proposal unacceptable deemed improper unequal discussions because revision was material); *Dubinsky v. United States*, 43 Fed. Cl. 243, 261 (1999) ("discussions with one offeror after the issuance of a request for final proposal revisions that enable it to make its proposal technically acceptable — as was the case here — are prohibited."); *Piquette & Howard Elec. Servs., Inc.*, B-408435.3, 2014 CPD ¶ 8 (Comp. Gen. Dec. 16, 2013) (permitting awardee to revise narrative regarding sequencing of work under a contract for replacement of fire alarm systems constituted a material revision to awardee's proposal transforming it from unacceptable to acceptable). *See also Standard Communications, Inc.*, B-406021, 2012 CPD ¶ 51 (Jan. 24, 2012) ("It is axiomatic that, if a concern makes a revision to its quote or proposal that has the effect of converting it from one that is unacceptable to one that is acceptable and eligible for award, the revision is material and discussions have occurred.")

REDACTED—FOR PUBLIC INSPECTION

But those cases do not help Neustar's cause. Here, Telcordia's proposal fully complies with the solicitation's existing security requirements. None of the FoNPAC, SWG, NANC nor the Commission contemplates such any relaxation of the solicitation's requirements — and Neustar does not claim otherwise. Rather, Neustar claims that the Commission must *add* requirements, not remove or relax them. Accordingly, the cases Neustar relies upon are simply inapplicable, and do not lead to the conclusion that the Commission must amend the solicitation and reopen discussions.

Perhaps recognizing the inapplicability of these cases, Neustar then cites another line of decisions involving situations where a federal agency made *material* changes to its requirements.¹³ But those cases articulate a detailed standard for assessing the materiality of a change to the agency's requirements, and the supposed "changes" that Neustar demands here do not meet that standard. Rather, all of Neustar's purported concerns are easily encompassed by the solicitation's existing requirements. And the development of a detailed plan for implementing the solicitation's existing security requirements during contract performance does not constitute a material change to requirements. Neustar thus cannot demonstrate that there has been any material change in requirements that would trigger a reopening of the competition (if, that is, this were a federal procurement).

¹³ As Neustar acknowledges in its Reply Comments, the restriction mandating competition as the result of a change in an agency's requirements is limited to "material changes" to ensure that the awarded contract is based upon competition for work that will actually be performed. Neustar Reply Comments at 71 n. 215.

REDACTED—FOR PUBLIC INSPECTION

When examining whether a contemplated revision to an agency's requirements is "material," both the Court of Federal Claims and the Government Accountability Office will consider whether the work to be performed under the contract is materially different than the work described in the solicitation.¹⁴ In making such an assessment, the Court and GAO consider factors such as "the extent of any changes in the *type of work, period of performance* and *costs* between the contract as awarded and modified."¹⁵

For example, a thirty-five percent reduction in the overall volume of work to be performed under a particular contract constituted a sufficiently material change to the contract requirements to justify cancellation of the original solicitation and recompetition based upon the agency's revised requirements.¹⁶ Similarly, a post-award modification of an awarded contract to remove over seventy percent of the work contemplated also constituted a material revision to the agency's requirements necessitating competition for the revised requirement.¹⁷ Likewise, where the composition of an agency's needs by the time of its award diverged substantially from the original solicitation requirements (causing an increase in one category of service and a decrease in another category of

¹⁴ See *Cardinal Maintenance, Inc. v. United States*, 63 Fed. Cl. 98, 106 (2004).

¹⁵ *Id.* (emphasis added) (citations omitted).

¹⁶ See *Naval Sys., Inc.*, B-407090.3, 2012 CPD ¶ 326 at 2 (Comp. Gen. Nov. 20, 2012).

¹⁷ See *System Studies & Simulation, Inc.*, B-409375.2, B-409375.3, 2014 CPD ¶ 153 (Comp. Gen. May 12, 2014).

REDACTED—FOR PUBLIC INSPECTION

work) such a substantial shift in the composition of the work constituted a material change.¹⁸

Here, there is no material change to the nature, scope, duration, or volume of the work Telcordia contemplates providing as the LNPA under the resulting contract. To the contrary, each of Neustar's supposed concerns fits easily within the security and ELEP framework of the existing solicitation. The solicitation sets forth a robust security framework, and the NAPM may reasonably supplement those requirements during implementation.

Neustar is complaining about a routine matter of contract administration. This solicitation — like any solicitation — stated its requirements at an appropriate level of generality. After the contract is awarded, Telcordia — like any awardee in a federal procurement — will work with the stakeholders to define the details of how it will implement its technical solution in the way that best meets their needs. That process is not only unobjectionable, but unavoidable. Such issues have nothing to do with the propriety of the agency's award decision under the terms of the solicitation. Rather, they are post-award contract administration issues the authority for which rests solely with the administering agency.¹⁹ Neustar has nothing to complain about.

¹⁸ *United Telephone Co.*, B-246977, 92-1 CPD ¶ 374 at 5-7 (Comp. Gen. Apr. 20, 1992).

¹⁹ *Chapman Law Firm v. United States*, 63 Fed. Cl. 519, 529-30 (2005), *aff'd* 163 Fed. Appx. 889 (Fed. Cir. 2006); *see also Aegis Assoc., Inc.*, B-238712 et al., May 31, 1990, 1990 WL 278045 at *1. *Northern Telecom Inc. v. United States*, 8 Cl. Ct. 376, 381

REDACTED—FOR PUBLIC INSPECTION

III. Telcordia's Ability to Satisfy Specified Security Criteria — Such as Possession of a Security Clearance — Concerns a Matter of Responsibility For Which Federal Procurement Law Permits Post-Selection Communications

Finally, even if the FCC chooses to apply federal procurement-law concepts, under federal procurement law, the question of whether an offeror is capable of satisfying security measures — such as obtaining security clearance — is considered a matter of contractor responsibility not subject to review in a bid protest.²⁰ As explained in Telcordia's Reply Comments, the FCC may request information relating to an offerors' responsibility without triggering the requirement to hold discussions with all offerors in the competitive range.²¹ This is because an agency's responsibility determination — *i.e.*, whether an offeror satisfies the standards outlines in FAR 9.104-1 regarding the contractor's ability to perform — is independent from the agency's assessment of the

(1985) (“protests...alleging that the awardee will not deliver equipment in conformance with contract requirements concern matters of contract administration, which are the responsibility of the contracting agency and which are not considered under our bid protest function.”).

²⁰ See *Ktech Corp.*, B-241808, B-241808.2, Mar. 1, 1991, 91-1 CPD ¶ 237 at 2 (“whether a prospective contractor has the ability to obtain any necessary security clearances concerns the firm's ability to perform and is therefore a matter of responsibility.”); see also *Rohmann Servs., Inc.*, B-405171, B-405171.2, Sept. 8, 2011, 2011 CPD ¶ 177 at 6 (“the ability to obtain a security clearance generally is a matter of responsibility, absent an express requirement in the solicitation to demonstrate the ability prior to award.”)

²¹ See Telcordia Reply Comments at 48 & n. 121 (citing *General Dynamics—Ordnance & Tactical Sys.*, B-295987, B-295987.2, 2005 CPD ¶ 114 at 10 (Comp. Gen. May 20, 2005)).

REDACTED—FOR PUBLIC INSPECTION

technical merits of the proposed awardee's proposal under the solicitation's evaluation criteria. Such exchanges regarding issues of responsibility can encompass a range of topics from organizational conflict of interest questions to other issues such as financial capacity or compliance with subcontracting requirements.²²

In the case of the LNPA solicitation, because the RFP contains no express requirement that the offerors must have a security clearance prior to award, there is nothing preventing the FCC from discussing whether Telcordia would be able to meet such a requirement in the context of a responsibility determination should the FCC decide that such clearances (or other security protections) are necessary.

IV. Neustar's Argument that the SWG and NANC Reports Violate the FACA Ignores the Law and is Wrong on the Merits

A. FACA's Fairly Balanced Requirement Does Not Apply to the SWG, and Even If It Did, the NANC and SWG Were Fairly Balanced.

Neustar's argument that the Commission cannot rely on the SWG report or the NANC recommendation because of alleged violations of the Federal Advisory

²² See *General Dynamics—Ordnance & Tactical Sys.*, B-295987, B-295987.2, 2005 CPD ¶ 114 at 10 (Comp. Gen. May 20, 2005) (finding agency's discussion with proposed awardee prior to award regarding small business subcontracting plan unobjectionable); *Overlook Sys. Tech.*, B-298099.4; B-298099.5, 2006 CPD ¶ 185 at 21 (Comp. Gen. Nov. 28, 2006) (agency's exchange regarding awardee's organizational conflict of interest mitigation plan permissible and is not require opening discussions with all offerors); *DaeKee Global Co. Ltd.*, B-402687.8, 2013 CPD ¶ 153 (Comp. Gen. Jan. 3, 2012) (communications regarding awardee's financial resources were not considered discussions and did not trigger the need to reopen discussions with all competitive range offerors).

REDACTED—FOR PUBLIC INSPECTION

Committee Act (“FACA”) ignores the law, and it is wrong on the merits. Neustar ignores that under the GSA’s rules, FACA requirements do not apply to *subcommittees* of advisory committees, like the SWG, when they report to a parent advisory committee which then undertakes further deliberations.²³ NANC did not simply rubber-stamp the SWG’s determinations; it conducted its own assessment of the SWG’s recommendations, and its ultimate recommendation was the product of its own deliberations. Therefore, under the GSA’s rules, FACA, including the fairly balanced requirement, does not apply to the SWG.

Neustar makes the stark claim that the SWG violated FACA’s “fairly balanced” requirement²⁴ simply because it “was composed mostly of large carriers and no consumer groups”²⁵ But even if the FACA’s “fairly balanced” requirement did apply to the SWG, Neustar has also waived this objection, and, ultimately, it is wrong that the SWG was not fairly balanced.

Neustar failed to object to the SWG’s composition when the group was created. In March 2011, Telcordia proposed that SWG membership be balanced between industry

²³ 41 C.F.R. § 102-3.35(a) (“In general, the requirements of the Act . . . do not apply to subcommittees of advisory committees that report to a parent advisory committee and not directly to a Federal officer or agency.”); *cf. id.* § 102-3.145 (excusing subcommittees from openness requirements unless recommendations will be adopted by parent committee or agency “*without further deliberations*” (emphasis added)).

²⁴ See 5 U.S.C. app. 2 § 5(b); 41 C.F.R. § 102-3.30(c).

²⁵ Neustar Reply Comments at 37-38.