Here, the FoNPAC and NAPM properly evaluated proposals in accordance with the terms of the RFP, and recommended award to Telcordia. It is entirely proper, and consistent with federal procurement principles, to proceed with award on that basis. Should NAPM, in consultation with the Commission, later decide that it is appropriate to modify its security specification post-award, it may negotiate such a modification with Telcordia, without revising the RFP or re-opening the competition.[307] That is because such issues have nothing to do with the propriety of the agency's evaluation and award decision under the terms of the solicitation. Rather, they are post-award contract administration issues, the authority for which rests solely with NAPM.[308]

In fact, here the RFP itself expressly contemplated that additional security measures would be developed and implemented post-award. ELEP is a prime example, because it will involve separate agreements with law enforcement to be negotiated and executed post-award.[309] And those agreements will necessarily alter the security requirements of the NAPM contract. As this example shows, NAPM has the authority to modify the awarded contract to incorporate any additional security requirements that may emerge without needing to re-compete the

---

[307] And to the extent that Neustar is questioning whether Telcordia will comply with the RFP's existing security requirements, that question also is a matter of contract administration, not subject to challenge under federal procurement rules. *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 (1985) ("[p]rotests. . . alleging that the awardee will not deliver equipment in conformance with the 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.").

[308] *Chapman Law Firm*, 63 Fed. Cl. at 529-30.

[309] RFP § 11.2.

requirement.[310] Because these issues are best addressed as post-award contract administration issues, the federal procurement principles upon which Neustar relies to assert a need to reopen the competition are wholly inapplicable.

B. Telcordia's Bid and Plans, Its Experience With U.S. National Security Protections, and Its International Experience All Demonstrate Its Ability to Develop and Implement a Highly Secure NPAC.

Nor do the security concerns now raised by Neustar's bid warrant any further delay in the process. As explained below, Telcordia's extensive experience shows that it is ready, willing, and able to operate a fully secure NPAC system and all related services. Telcordia has proposed, and plans, a robust set of security protections, and many of the specific issues raised by Neustar are predicated on factual inaccuracies. And to the extent that the relevant Executive Branch agencies determine that additional assurances are appropriate, these can and should be addressed through post-selection mitigation with the relevant agencies. Telcordia is willing to make any reasonable assurances with appropriate Executive Branch agencies a condition of it's LNPA selection—which would put it on a par with maintaining neutrality, which is an ongoing requirement.

1. Telcordia Has Substantial Experience in Operating Reliable and Secure Databases

a. Telcordia Has Experience in U.S. National-Security Protections.

Like Neustar, Telcordia is an American company, with deep roots that go back to the fabled Bell Labs. ****BEGIN CRITICAL INFRASTRUCTURE** **BEGIN HIGHLY CONFIDENTIAL **** [redacted]

[310] Neustar comments at 116 n.314.

[redacted] ****END HIGHLY CONFIDENTIAL** **END CRITICAL INFRASTRUCTURE****

As the FCC is aware, not the least from its own authorization and licensing process, companies that provide highly complex systems and technologies of great criticality to U.S. national security, national defense, and homeland security routinely adopt U.S.-defined protections. The United States has a system with strong protections, and ****BEGIN CRITICAL INFRASTRUCTURE** **BEGIN HIGHLY CONFIDENTIAL **** [redacted] ****END HIGHLY CONFIDENTIAL** **END CRITICAL INFRASTRUCTURE**** Moreover, Telcordia already provides products and services critical to telephone routing, including Telcordia Routing Administration (i.e. LERG) and Common Language services.

b. Telcordia's International Experience Is a Strength.

Telcordia's home base is the United States, ****BEGIN CRITICAL INFRASTRUCTURE**** [redacted]

[redacted] ****END CRITICAL INFRASTRUCTURE**** Those 20 countries include five NATO countries, Canada, and Mexico, and all of the countries where Telcordia provides these services are members of the World Trade Organization.

Telcordia LNPA systems in other countries have security procedures. ****BEGIN CRITICAL INFRASTRUCTURE** **BEGIN HIGHLY CONFIDENTIAL **** [redacted] ****END HIGHLY CONFIDENTIAL** **END CRITICAL INFRASTRUCTURE****

2. Telcordia Is Ready, Willing, and Able to Meet All Security Needs.

Telcordia and its data center partner, Sungard AS, are completely capable of and committed to meeting all of the security requirements envisioned by the RFP for both the NPAC/SMS system and the ELEP. Telcordia, and Sungard AS, will steadfastly remain compliant with the security requirements outlined in the RFP, as well as any security requirements agreed to in post-selection mitigation, recognizing that these are flexible enough to account for changes in the threat environment. ****BEGIN CRITICAL**

INFRASTRUCTURE **BEGIN HIGHLY CONFIDENTIAL **** [redacted]

****END HIGHLY CONFIDENTIAL** **END CRITICAL INFRASTRUCTURE****

Moreover, as explained in Part I.B.2.c, *supra*, in its bid, Telcordia has also agreed to implement numerous safeguards to ensure its independence of Ericsson, and these safeguards further mitigate any national-security issues posed by Ericsson's acquisition of Telcordia. For example, as explained earlier, Telcordia will have its own board of directors, a majority of whom will be outside independent directors. Indeed, Telcordia's five-member board will have only *one* Ericsson representative; the remaining four members are U.S. citizens.

Furthermore, Telcordia is aware of and experienced in a dynamic threat environment, especially in view of the prevalence of Chinese and other national, sub-national, and criminal intrusions and attacks over the last few years and the post-Snowden revelations. Telcordia is willing to be required, as a condition of its selection as LNPA, to provide reasonable assurances to the appropriate U.S. Executive Branch agencies. Based on its deep experience with mission critical telecommunications infrastructure and systems, Telcordia is confident that it will meet all the requirements and standards to be a fully secure LNPA provider, perhaps adding more security features and experience than has been afforded to the Nation in the past.

****BEGIN CRITICAL INFRASTRUCTURE** **BEGIN HIGHLY CONFIDENTIAL ****

[redacted]

[redacted]

[redacted]

[redacted] **END

HIGHLY CONFIDENTIAL** **END CRITICAL INFRASTRUCTURE**

3. Many of the Security "Issues" Raised by Neustar Are Simply Wrong on the Facts.

Despite the strength of Telcordia's bid and its extensive experience, Neustar has, in the press[311] and in its reply comments, dreamed up a number of supposed security issues. The majority of these issues are simply wrong on the facts. First, contrary to Neustar's assertions, Telcordia is not re-using code from foreign implementations. The code for the NPAC is being developed from scratch in America. Similarly, contrary to reports in the press, there is no danger that hackers could "hack into the database to see what numbers the FBI or another security agency has wiretaps on."[312] The NPAC does not keep records of which numbers are the subject of law-enforcement inquiries via ELEP, so there are simply no records for a hacker to steal. The other ELEP concerns raised by Neustar are similarly meritless. Finally, Ericsson's BSS/OSS products cannot, under the RFP, and will not be integrated into the NPAC.

a. Telcordia Is Not Reusing Code from Foreign Implementations, and the NPAC's Operations Will Be In, by, and For America.

In the press, Neustar has suggested that Telcordia is reusing code from number-portability systems in foreign countries. This is entirely false. Telcordia is creating entirely new code for the U.S. NPAC, developed in America. Telcordia is not re-using code from foreign

---

[311] At the same time that Neustar was redacting pages of security hysteria in its Comments for the FCC, its officers and agents were discussing many of those concerns in the press. Indisputably, this Janus-like approach to security is a clear indicator that Neustar merely and mercenarily desires to exploit the U.S. Government's legitimate concern about the security as a foil and an artifice to achieve what it could not in the selection process.

[312] Ellen Nakashima, *Neustar, Telcordia Battle Over FCC Contract to Play Traffic Cop for Phone Calls, Texts,* Wash. Post (August 9, 2014), http://www.washingtonpost.com/world/national-security/neustar-telcordia-battle-over-fcc-contract-to-play-traffic-cop-for-phone-calls-texts/2014/08/09/778edeaa-1e7b-11e4-ae54-0cfe1f974f8a_story.html.

implementations, nor is it contracting its code development from non-U.S. sources. All NPAC user data will be stored in the continental United States in dedicated servers and equipment with physical and logical access control. ****BEGIN CRITICAL INFRASTRUCTURE** **BEGIN HIGHLY CONFIDENTIAL **** [redacted] ****END HIGHLY CONFIDENTIAL** **END CRITICAL INFRASTRUCTURE** Neustar's** comments to the contrary are speculative nonsense.

Telcordia's LNPA service does not and will not reuse any code from existing Telcordia LNP applications. ****BEGIN CRITICAL INFRASTRUCTURE** **BEGIN HIGHLY CONFIDENTIAL **** [redacted] ****END HIGHLY CONFIDENTIAL** **END CRITICAL INFRASTRUCTURE**** The application is being developed new *from scratch* using the existing industry requirements (*e.g.* FRS, IIS, and XIS).

****BEGIN CRITICAL INFRASTRUCTURE** **BEGIN HIGHLY CONFIDENTIAL **** [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted] ****END HIGHLY CONFIDENTIAL** **END CRITICAL INFRASTRUCTURE****

b. Telcordia Can and Will Meet All Enhanced Law Enforcement Platform Requirements.

In addition to the fact that Neustar's complaints about the RFP's handling of the Enhanced Law Enforcement Platform and its security are an untimely attempt to re-hash the selection process, Neustar is factually incorrect. The RFP does not ignore ELEP. Rather, the RFP covers it significantly, and, in fact, includes security-related requirements for ELEP.[313] Telcordia has responded substantively and demonstrated that it has the experience and capability to ensure a smooth transition, assuming Neustar's cooperation, and to provide continuous, stable ELEP services.

[313] *See generally* 2015 LNPA RFP § 11.2 (RFP); *id.* § 11.2, REQ 8 ("Access to Enhanced Law Enforcement Platform shall be accomplished by authenticated, secure and encrypted means.").

****BEGIN CRITICAL INFRASTRUCTURE** **BEGIN HIGHLY CONFIDENTIAL****

****END CONFIDENTIAL** **END CRITICAL INFRASTRUCTURE****

In any case, Neustar's Chicken Little claims regarding ELEP[314] are wrong on the merits. Telcordia's process would not retain queries made by law enforcement agencies using ELEP. Telecommunications providers are required to maintain records of requests for law enforcement access, but those requirements do not apply to Telcordia in its administration of the NPAC. Further, Telcordia's ELEP administrator and other personnel would not be allowed to monitor law enforcement queries. Additionally, the RFP adequately requires[315] a separate agreement between the NPAC/SMS operator and law enforcement.

****BEGIN CRITICAL INFRASTRUCTURE** **BEGIN HIGHLY CONFIDENTIAL****

[314] Ellen Nakashima, *Neustar, Telcordia Battle Over FCC Contract to Play Traffic Cop for Phone Calls, Texts,* Wash. Post (August 9, 2014), http://www.washingtonpost.com/world/national-security/neustar-telcordia-battle-over-fcc-contract-to-play-traffic-cop-for-phone-calls-texts/2014/08/09/778edeaa-1e7b-11e4-ae54-0cfe1f974f8a_story.html.

[315] RFP § 11.2, REQ 5, REQ 16.

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted] **END CRITICAL INFRASTRUCTURE**

c. **The NPAC Will Not Be Integrated With BSS/OSS Products.**

BEGIN CRITICAL INFRASTRUCTURE [redacted]

[redacted]

[redacted]

[redacted]

[redacted] ****END CRITICAL INFRASTRUCTURE****

The NPAC cannot technically treat any one carrier's OSS/BSS systems differently than the others. The carrier OSS/BSS systems are not co-resident with or connected to the NPAC. The OSS/BSS systems interface to the NPAC through gateway products (SOA, LSMS) that have to comply with industry-defined standard protocols that designate the specific messages associated with the features that are supported by the NPAC. All features supported by the NPAC are standard for all carriers and managed through an industry change management process supervised by the LNPA WG, which is a working group reporting into the NANC. The LNPA can only implement technical changes after they are accepted by the LNPA WG and approved by the NAPM LLC, as contract administrator. Both groups report into NANC, which oversees the NPAC system.

The Telcordia NPAC will only perform the agreed-upon NPAC features and functions that are defined by the industry specifications managed through the industry working groups and the designated FCC contract manager, NAPM LLC. No other functionality will be included in the NPAC. If Ericsson ever desires to become a user of the NPAC, it would have to apply and go through the same approval process as any other user, a process that would be completely transparent and open to the U.S. Government. There would be no possibility of integration, no back door, and no partiality.

d. The Emergency Communications Concerns Raised by Neustar Would Require a Series of Complex Intrusions, Which Telcordia Has Safeguards to Prevent.

****BEGIN CRITICAL INFRASTRUCTURE****

****END HIGHLY CONFIDENTIAL** **END CRITICAL INFRASTRUCTURE****

C. Telcordia Is Already Consulting With National Security and Law-Enforcement Agencies to Address Post-Selection Implementation Issues.

Finally, to the extent that any security issues remain, these are appropriately handled through post-selection mitigation with the appropriate agencies. As explained above, Telcordia has already proposed and further plans a robust set of security protections and has extensive experience addressing national-security concerns of relevant government agencies. To the extent that the relevant agencies determine that additional protections are necessary, Telcordia is ready, willing, and able to address these through post-selection discussions with the relevant agencies. Indeed, Telcordia is already consulting with the relevant agencies to address post-selection implementation issues.

The Commission should not delay selection while those discussions occur. As explained already, Telcordia is willing to make any reasonable assurances with appropriate Executive Branch agencies as a condition of LNPA selection—which would put it on a par with maintaining neutrality, which is an ongoing requirement. Given Telcordia's extensive experience, there should be no doubt that Telcordia will be able to secure and protect the NPAC and to give any reasonable assurances to the relevant agencies. The Commission should not allow that process to hold up a selection decision, which can be reached expeditiously on the current record.

* * *

The FCC in its RFP recognized the grave importance of security to the NPAC and its ELEP function, requiring details and yet the flexibility to assure the agility of the LNPA to meet existing and future security needs and concerns. Telcordia substantively responded in detail, incorporating its experiences worldwide while making the NPAC an American creation on

American soil. ****BEGIN CONFIDENTIAL****

****END CONFIDENTIAL**** Neustar has thrown out so many red herrings to distract logical decision making and straw men against which to tilt that they may have obscured one other fact: Neustar has not provided any substantive basis for overturning the recommendation based on security. Indeed, Telcordia not only can do as well as Neustar at protecting the security of the NPAC, but with its new build it may do much better.

CONCLUSION

The Commission should approve the NANC's recommendation of Telcordia as the next LNPA and should direct NAPM to expeditiously enter a contract with Telcordia.

Respectfully submitted,

John T. Nakahata
Christopher J. Wright
Amy E. Richardson
Mark D. Davis
Randall W. Sifers
Kristine Laudadio Devine
Stephen W. Miller
Anne K. Langer
John R. Grimm
HARRIS, WILTSHIRE & GRANNIS LLP
1200 18th Street, N.W. Suite 1200
Washington, D.C. 20036
(202) 730-1320
jnakahata@harriswiltshire.com

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

August 22, 2014

Exhibit A

Declaration of Travis Baker

REDACTED--FOR PUBLIC INSPECTION

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	WC Docket No. 09-109
Telephone Number Portability	CC Docket No. 95-116

DECLARATION OF TRAVIS BAKER

My name is Travis Baker. I am Director, Deployment & Integration, at Ericsson Inc. I have personal knowledge of the information in this declaration.

1) Ericsson Inc. provides managed services to a range of telecommunications customers in the United States.

2) These MSAs are not joint ventures and do not include revenue-sharing agreements. Rather, they are arms-length contractual relationships.

3) Ericsson Inc. has MSAs with ****BEGIN HIGHLY CONFIDENTIAL**** [redacted] ****END HIGHLY CONFIDENTIAL**** telecommunications services providers.

4) The Managed Services Agreement by and Between Sprint/United Management Company And Ericsson Inc. formerly known as Ericsson Services Inc. ("2009 Sprint MSA") is no longer in effect. It has been superseded by an Amended and Restated Managed Services Agreement by and Between Sprint/United Management Company and Ericsson Inc., ("Current Sprint MSA") effective July 2013.

5) At the time it was in effect, the 2009 Sprint MSA stated that Ericsson and Sprint remained completely independent entities and were not ****BEGIN HIGHLY CONFIDENTIAL**** [redacted] ****END HIGHLY CONFIDENTIAL**** Ericsson Services Inc., as supplier, was responsible for ****BEGIN HIGHLY CONFIDENTIAL**** [redacted] ****END HIGHLY CONFIDENTIAL**** It also had ****BEGIN HIGHLY CONFIDENTIAL**** [redacted] ****END HIGHLY CONFIDENTIAL****

6) The Current Sprint MSA contains the same provisions.[4]

7) The Current Sprint MSA requires Ericsson Inc. to abide by certain ****BEGIN HIGHLY CONFIDENTIAL**** [redacted] ****END HIGHLY CONFIDENTIAL**** But again, the contract makes clear that these policies all involve Ericsson Inc.'s *performance of services for Sprint* or conduct *while on Sprint property*—for example, ****BEGIN HIGHLY CONFIDENTIAL**** [redacted]

---

1 Managed Services Agreement by and Between Sprint/United Management Company And Ericsson Services Inc.§ 19.12 (July 7, 2009) ("2009 Sprint MSA").

2 *Id.*

3 *Id.*

4 Amended and Restated Managed Services Agreement by and Between Sprint/United Management Company and Ericsson Inc. § 19.12 (July 2013) ("2013 Sprint MSA").

5 2009 Sprint MSA § 17.1 (emphasis added).

[redacted]

[redacted] **END HIGHLY CONFIDENTIAL**

8) The 2009 Sprint MSA and the Current Sprint MSA provide:

BEGIN HIGHLY CONFIDENTIAL [redacted] **END HIGHLY CONFIDENTIAL**

9) Ericsson Inc. previously had an MSA with Clear Wireless LLC, but that agreement is no longer in effect.

10) After Sprint acquired Clear Wireless, the MSA between Clearwire and Ericsson Inc. was terminated and merged with the Current Sprint MSA.

---

[6] *Id.*

[7] *Id.* § 19.12 (emphasis added).

11) The Current Sprint MSA provides that responsibility for certain **BEGIN HIGHLY CONFIDENTIAL** [redacted] **END HIGHLY CONFIDENTIAL** is transferred back to Sprint.[9] The contract states: **BEGIN HIGHLY CONFIDENTIAL** [redacted] **END HIGHLY CONFIDENTIAL**

12) **BEGIN HIGHLY CONFIDENTIAL** [redacted] **END HIGHLY CONFIDENTIAL**

13) When Ericsson Inc. had numbering responsibilities in the 2009 Sprint MSA, those responsibilities never included number portability or involved submitting any requests to the NPAC. To the extent that Ericsson Inc. had responsibility for numbering at all, its responsibilities never required it to initiate transactions with the Number Portability Administration Center ("NPAC"), nor did its contractual duties depend on its ability to successfully port a number through the NPAC or to obtain a certain result from the Local Number Portability Administrator.

I declare under penalty of perjury that the foregoing is true and correct.

Executed: August 7, 2014

Travis Baker

---

8 2013 Sprint MSA, Ex. B at 16.

9 *Id.* at 3 (Recitals ¶B).