

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20544

In the Matter of

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

COMMENTS OF NEUSTAR, INC.

Brendan V. Sullivan, Jr.
David D. Aufhauser
Beth A. Stewart
WILLIAMS & CONNOLLY
725 12th Street, N.W.
Washington, D.C. 20005
(202) 434-5000

Stewart A. Baker
Kaitlin Cassel
STEPTOE & JOHNSON LLP
1330 Connecticut Avenue, N.W.
Washington, D.C. 20036
(202) 429-3000

Thomas J. Navin
Nancy J. Victory
Tyrone Brown
Brett Shumate
WILEY REIN LLP
1776 K Street, N.W.
Washington, D.C. 20006
(202) 719-7000

July 25, 2014

Aaron M. Panner
Evan T. Leo
Melanie L. Bostwick
KELLOGG, HUBER, HANSEN, TODD,
EVANS & FIGEL, P.L.L.C.
1615 M Street, N.W., Suite 400
Washington, D.C. 20036
(202) 326-7900

Leonard J. Kennedy
Scott M. Deutchman
J. Beckwith Burr
Richard L. Fruchterman, III
Aaron N. Goldberger
NEUSTAR, INC.
1775 Pennsylvania Avenue, N.W.
4th Floor
Washington, D.C. 20006
(202) 533-2705

Michele Farquhar
Praveen Goyal
HOGAN LOVELLS US LLP
555 13th Street, N.W.
Washington, D.C. 20004
(202) 637-5600

TABLE OF CONTENTS

	Page
INTRODUCTION AND EXECUTIVE SUMMARY.....	2
I. ERICSSON IS NOT IMPARTIAL AND WOULD NOT BE A NEUTRAL NUMBERING ADMINISTRATOR	13
A. Ericsson’s Contractual and Vendor Relationships with Major Wireless Providers Disqualifies Its Subsidiary from Serving As LNPA.....	14
1. Ericsson – Parent and Subsidiary – Is Subject To Undue Influence.....	14
2. Ericsson’s Subsidiary Is Barred from Serving As LNPA Because It Is an Affiliate of a Telecommunications Network Equipment Manufacturer ...	33
B. SunGard Is Not a Neutral Third Party Because of Its Affiliation with Various IVPs and TSPs	35
1. SunGard Is an Affiliate of an Interconnected VoIP Provider and at Least Two Telecommunications Service Providers	36
2. SunGard Is Subject to Undue Influence Because of Its Private Equity Owners’ Interest in an Interconnected VoIP Provider.....	40
3. No Safeguards Could Make SunGard Impartial or Able To Meet the Commission’s Neutrality Requirements	42
C. Neutrality Requirements Play a Critical Role in Ensuring the Effective Functioning of the NPAC	46
D. The NANC Recommendation Fails To Address Neutrality; in Any Event, the Issue Is for the Commission To Resolve	47
II. THE COMMISSION CANNOT DESIGNATE A NEW ENTITY TO SERVE AS LNPA WITHOUT A NOTICE OF PROPOSED RULEMAKING.....	50
A. The Designation of Impartial Numbering Administrators Pursuant to Section 251(e)(1) Requires Notice-and-Comment Rulemaking.....	51
B. Designation of Ericsson as LNPA Would Constitute a Change of a Rule Adopted Pursuant to a NPRM Published in the Federal Register and Requires the Same Procedure	55
C. A Notice of Proposed Rulemaking Is Required To Ensure Interested Parties Can Comment Effectively on a Major Change to the Nation’s Basic Telecommunications Infrastructure	61

**SECOND CORRECTED COPY
REDACTED – FOR PUBLIC INSPECTION**

III.	FLAWS IN THE SELECTION PROCESS PRECLUDE THE COMMISSION FROM RELYING ON THE NANC’S RECOMMENDATION	63
A.	The Commission Cannot Delegate the Choice of LNPA to the NANC	63
B.	Flaws in the NANC’s Process Precluded Submission of the Most Favorable Available Proposals	65
IV.	THE COMMISSION CANNOT REASONABLY RELY ON THE NANC/NAPM RECOMMENDATION BECAUSE IT FAILS TO JUSTIFY THE SELECTION OF ERICSSON	76
A.	The Recommendation Does Not Adequately Address the Transition Risks	78
B.	The Recommendation Flouts the RFP by Largely Ignoring Technical and Management Criteria in Favor of Price	82
C.	[BEGIN CONFIDENTIAL INFORMATION] [REDACTED] [REDACTED] [END CONFIDENTIAL INFORMATION].....	84
D.	The Recommendation Fails To Scrutinize Ericsson’s Service Quality Commitments.....	88
E.	The Recommendation Fails To Account for IP Transition Issues	89
V.	ERICSSON’S TRANSITION PLAN IS INADEQUATE AND WILL IMPOSE UNACCEPTABLE RISKS.....	92
VI.	NATIONAL SECURITY ISSUES ARE NOT ADEQUATELY ADDRESSED IN THE EXISTING RFP AND ARE A BASIS ON WHICH THE CANDIDATES MUST COMPETE.....	102
A.	The Selection of an LNPA Raises Serious National Security Issues.....	102
1.	LEAP.....	102
2.	Emergency communications.....	103
3.	Differences in the candidates’ security profile.	104
B.	Security Has Not Yet Been Properly Considered in the Selection Process	107
1.	The RFP’s security terms.....	107
2.	The security terms required in similar contexts.....	108

**SECOND CORRECTED COPY
REDACTED – FOR PUBLIC INSPECTION**

3. Recent security developments call for a greater priority for security..... 111

C. This Is the Time To Consider Security Fully in Choosing the LNPA..... 112

CONCLUSION..... 116

VI. NATIONAL SECURITY ISSUES ARE NOT ADEQUATELY ADDRESSED IN THE EXISTING RFP AND ARE A BASIS ON WHICH THE CANDIDATES MUST COMPETE

The selection of an LNPA implicates serious national security issues that were not addressed in the RFP process.²⁹³ Without proper vetting, these issues raise significant questions as to the vulnerability of critical U.S. telecommunications infrastructure under a new LNPA and represent a serious deficiency in the process and substance of the selection competition.²⁹⁴ The Commission can cure this deficiency by conferring with the Executive Branch, adopting a set of minimum security requirements, and allowing the candidates to compete on the relative security of their proposed systems.

A. The Selection of an LNPA Raises Serious National Security Issues

[BEGIN NATIONAL SECURITY INFORMATION] [REDACTED]

[REDACTED] **[END NATIONAL SECURITY INFORMATION]**

1. LEAP. [BEGIN NATIONAL SECURITY INFORMATION] [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

²⁹³ As noted above, *see supra* n.214, Despite Neustar’s request for appropriate representatives to receive access to information redacted for national security reasons, Neustar has had no access to the elements of Ericsson’s proposal that have been redacted for such reasons, and its comments are therefore necessarily incomplete.

²⁹⁴ *See generally* 47 U.S.C. § 151 (creating the Commission “for the purpose of the national defense, [and] for the purpose of promoting the safety of life and property through the use of wire and radio communications,” among other purposes).

[REDACTED]

[REDACTED] [END NATIONAL SECURITY

INFORMATION]

2. Emergency communications. [BEGIN NATIONAL SECURITY

INFORMATION] [REDACTED]

[REDACTED]

²⁹⁵ See Exec. Order No. 13,618, § 5.1, 77 Fed. Reg. 40,779, 40,780-81 (July 11, 2012) (“The Secretary of Defense shall: (a) oversee the development, testing, implementation, and sustainment of NS/EP communications that are directly responsive to the national security needs of the President, Vice President, and senior national leadership, including: communications with or among the President, Vice President, White House staff, heads of state and government, and Nuclear Command and Control leadership; Continuity of Government communications; and

[REDACTED]

[REDACTED] [END NATIONAL SECURITY INFORMATION]

3. Differences in the candidates’ security profile. The two number portability competitors’ business models are also different in ways that present different security risk profiles.

a. Ericsson as a multipurpose outsourcer for telecommunication carriers.

Ericsson wants to be an outsourced provider of many services to telecommunications operators – so many services, in fact, that it is not unfair to call Ericsson a “shadow” carrier. For example, it

communications among the executive, judicial, and legislative branches to support Enduring Constitutional Government.”). This responsibility has been transferred to DGS Office of Emergency Communications (DHS-EOC).

currently maintains and operates the switched network for Sprint²⁹⁶ and is hoping to do the same for Verizon and AT&T.²⁹⁷ It seeks to increase the dependence of operators on its services, and to use its existing and proposed services to enhance its access to operators' business operations. This strategy raises questions about Ericsson's neutrality, as discussed earlier, but it also affects Ericsson's plan for delivering number portability services. That is because strict application of the neutrality requirements for the LNPA has maintained a sharp division between the LNPA and carrier systems themselves, minimizing the risk that the LNPA will itself be a vector for infection of multiple carriers. Any breakdown in the neutrality requirements would therefore require addressing a series of national security concerns that have been avoided to date.

For example, in keeping with its outsourcing strategy, **[BEGIN NATIONAL SECURITY INFORMATION]** [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

²⁹⁶ Larry Dignan, *Sprint Outsources Network to Ericsson*, CNET, July 10, 2009, <http://www.cnet.com/news/sprint-outsources-network-to-ericsson>.

²⁹⁷ Adam Ewing, *Ericsson Talks to U.S. Mobile Carriers Over Managed Services*, BLOOMBERG, July 1, 2014, <http://www.bloomberg.com/news/2014-07-01/ericsson-in-talks-to-manage-wireless-networks-for-at-t-verizon.html>. As noted above, *see* p. 18, Ericsson has also signed a long-term managed services agreement with T-Mobile. *See* Sue Marek, *Ericsson CEO Says AT&T, Verizon Unlikely to Outsource Network Management*, FIERCEWIRELESSTECH, July 17, 2014, <http://www.fiercewireless.com/tech/story/ericsson-ceo-says-att-verizon-unlikely-outsource-network-management/2014-07-17>.

²⁹⁸ *See* iconective White Paper, *Best Practices for Number Portability Success* (Oct. 2011), available with registration at <http://iconectiv.com/iforms/whitepapers/best-practices-number-portability.php>.

[REDACTED]

[REDACTED] [END

NATIONAL SECURITY INFORMATION]

b. **Ericsson’s global footprint.** Ericsson is a Swedish company that operates, sources software and equipment, and sells goods and services in dozens of countries. In particular, it sells number portability software and services to many countries, including India, Pakistan, the UAE, and Saudi Arabia.²⁹⁹ In contrast, Neustar predominantly serves North America, and its software and systems are developed and maintained in the United States. These are important differences from the standpoint of national security. **[BEGIN NATIONAL**

SECURITY INFORMATION] [REDACTED]

[REDACTED]

²⁹⁹ See Telcordia, *Engaging MNP Management Solutions that Work for your Network*, Nov. 2012. India has been sufficiently concerned about national security risks that it has imposed mitigation requirements on Ericsson. See Rajat Guha, *Telcordia Tech Secures FIPB Nod to Manage Mobile Number Portability*, THE FINANCIAL EXPRESS, Nov. 8, 2010.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] [END NATIONAL SECURITY INFORMATION]

These are all questions that should be part of a security evaluation. [BEGIN NATIONAL SECURITY INFORMATION] [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[END NATIONAL SECURITY INFORMATION]

B. Security Has Not Yet Been Properly Considered in the Selection Process

For all these reasons, security should be at the center of the number portability selection process. But, in fact, it has not yet been seriously considered. The RFP reflects little or no direct federal or national security expertise. Only now has the selection process reached the federal level, where the Commission can consult officials with national security expertise and responsibilities.

1. The RFP's security terms. The inadequacy of the RFP from a security point of view is plain when it is compared to the security requirements imposed in comparable contexts. In general, the RFP contains few terms relating to the security of the number portability system.

In fact, all of the contract’s requirements are contained in three sections: RFP § 6.7, RFP § 9.20-21, and TRD § 7. These sections require the administrator to maintain and enforce adequate data center safety and physical security procedures; maintain and store the servers, data centers, and user data in the continental United States; monitor and record unauthorized system access and remedy logon security permission errors; restrict user access and maintain a system of authentication; generate audit logs; and have an intrusion detection and reporting system. *See* 2015 LNPA RFP §§ 6.7, 9.20-21; 2015 LNPA TRD § 7.

2. The security terms required in similar contexts. The previous requirements may appear comprehensive, but they are insufficient when compared to the requirements imposed by the Executive Branch and by Congress when national security and the telecommunications infrastructure are at stake.

a. Committee on Foreign Investment in the United States (CFIUS) and Team Telecom. If Ericsson had proposed to purchase Neustar or if it had applied to be a telecommunications operator in its own name, the Executive Branch agencies responsible for national security would have imposed detailed and comprehensive security requirements. CFIUS agencies concerned with security routinely negotiate mitigation agreements with foreign purchasers of critical U.S. infrastructure.³⁰⁰ And, relying on the Commission’s deference to the Executive Branch on national security matters, these same agencies insist that extensive security conditions be incorporated into the licenses allowing foreign companies to provide telecommunications service in the United States.³⁰¹

³⁰⁰ 50 U.S.C. app. § 2170(l).

³⁰¹ The Commission “regularly refers” requests to the Executive Branch’s Team Telecom and grants “those agencies *de facto* authority to disallow a transaction unless and until any national security concerns have been addressed.” The Commission also allows Team Telecom to

These security conditions include requirements such as a screening process for persons with direct or indirect access to the NPAC system; a U.S. citizen to serve as a full-time Security Compliance Officer and a U.S. citizen to serve as a full-time Technical Security Officer; a written security plan addressing physical, cyber, supply chain, and personal security; annual third-party audits of compliance with the security plan; annual and incident reporting requirements to the U.S. government regarding implementation and compliance with the security plan; prohibitions on “write” access or administrator access from outside the United States; prohibitions on non-U.S. citizens’ access to the source code used to administer the NPAC system; auditing and cooperation requirements by the U.S. government for any code utilized or developed in connection with the number portability system in the United States; U.S. government access to the LNPA’s facilities, records, personnel, and source code; and U.S. government approval of any contract to provide number portability services outside of the United States.³⁰² No terms such as these can be found in the RFP.

In addition, it is common for CFIUS and the Commission’s security agreements to include provisions protecting the investigative interests of law enforcement. Given the importance of LEAP in law enforcement and national security investigations, the RFP should

intervene on its own motion, which Team Telecom frequently does. And, where these agencies have “concerns about potential national security implications of a transaction, they typically require the transaction parties to enter into national security agreements as a condition of approval. These requirements, in turn, are relevant to the Commission’s ultimate determination whether the proposed investment would disserve the public interest.” *See* Public Notice, *Media Bureau Announces Filing of Request for Clarification of the Commission’s Policies and Procedures Under 47 U.S.C. § 310(b)(4) by the Coalition for Broadcast Investment*, 28 FCC Rcd 1469, 1486 (2013).

³⁰² *See, e.g.*, Agreement between Level 3 Communications, Inc. and the U.S. Department of Justice, the U.S. Department of Homeland Security, and the U.S. Department of Defense (Sept. 26, 2011), available at http://licensing.fcc.gov/myibfs/download.do?attachment_key=918724.

contain provisions protecting law enforcement’s interests in LEAP. In fact, it does not. Rather than insist on detailed protections for LEAP, the RFP suggests that providing LEAP services is a low priority. For example, the RFP states that the “Enhanced Law Enforcement Platform Service is discretionary and elective . . . and is not necessary” and that the “LNPA shall ensure that the Enhanced Law Enforcement Platform Service does not adversely affect the operation and performance of the NPAC/SMS, and any adverse effect shall be cause for termination” of LEAP. 2015 LNPA RFP § 11.2.

b. Security requirements in federal services and contracting. If the Commission supplied number portability services – or if it had directly issued an RFP to obtain portability services under a federal contract – it would be required by Congress to incorporate numerous security terms. This requirement originates from the Federal Information Security Management Act (“FISMA”) of 2002,³⁰³ under which the National Institute of Standards and Technology (“NIST”) has developed standards and minimum information security requirements for information and information systems collected or maintained by or on behalf of each federal agency. NIST published these standards as the Federal Information Processing Standards Publication 200 (“FIPS PUB 200”).

The FIPS PUB 200 standards apply to “all information within the federal government” and “all federal information systems” other than those designated as national security systems, which are subject to even more rigorous security requirements. FIPS PUB 200 at iv. These “minimum standards” are required to protect the “confidentiality, integrity, and availability of federal information systems and the information processed, stored, and transmitted by those systems.” *Id.* § 3. These minimum security requirements cover 17 security-related areas,

³⁰³ 44 U.S.C. § 3541 *et seq.*

including access control, awareness and training, certification, accreditation, and security assessments, contingency planning, incident response, risk assessment, and systems and communication protection. *Id.* Few or none of the security specifications required by FIPS PUB 200 are incorporated into the RFP.

3. Recent security developments call for a greater priority for security. Even if the national security concerns discussed above were not obvious when the RFP was drafted, they are essential to protecting the American people. Recent developments have shown that there are many people and governments interested in attacking the U.S. critical infrastructure.³⁰⁴ These attacks go beyond stealing information, focusing as well on causing failure that will be devastating to ordinary Americans.³⁰⁵ It has become common practice for hackers, state-sponsored or not, to use indirect means to gain access to targets.³⁰⁶ Sometimes that leads attackers to add defects directly to code as it comes from the supplier.³⁰⁷ Attackers have also

³⁰⁴ See Ellen Nakashima, *Indictment of PLA Hackers is Part of Broad U.S. Strategy to Curb Chinese Cyberspying*, WASH. POST, May 22, 2014 (discussing indictment of five members of the Chinese People’s Liberation Army for hacking and China’s “growing campaign of commercial cyberspying”), http://www.washingtonpost.com/world/national-security/indictment-of-pla-hackers-is-part-of-broad-us-strategy-to-curb-chinese-cyberspying/2014/05/22/a66cf26a-e1b4-11e3-9743-bb9b59cde7b9_story.html.

³⁰⁵ See Ian Urbina, *Hacker Tactic: Holding Data Hostage*, N.Y. TIMES, June 21, 2014 (discussing new tactics of hackers including ransomware to hold computer data hostage, and viruses that enable them to remotely wipe a hard drive clean or cause it to overheat), <http://www.nytimes.com/2014/06/22/sunday-review/hackers-find-new-ways-to-breach-computer-security.html>.

³⁰⁶ For example, hackers recently infected with malware the online menu at a Chinese restaurant popular with a big oil company’s employees in order to gain access to the business’ computer network. Similarly, hackers in the recent Target payment card breach gained access indirectly through its heating and cooling system. See Nicole Perlroth, *Hackers Lurking in Vents and Soda Machines*, N.Y. TIMES, Apr. 7, 2014, http://www.nytimes.com/2014/04/08/technology/the-spy-in-the-soda-machine.html?_r=0.

³⁰⁷ See Eduard Kovacs, *Hackers Attack Shipping and Logistics Firms Using Malware-Laden Handheld Scanners*, SECURITY WEEK, July 10, 2014 (discussing attack on shipping and logistic

begun exploiting a victim’s social graph to send emails pretending to be from a friend or coworker whose attachments and links are more likely to be trusted by the target.³⁰⁸

Consequently, no matter the view of the NAPM and the NANC on national security issues at the time the RFP was drafted, today it is plainly necessary to ask detailed security questions and to include detailed security requirements in the selection process of the LNPA.

C. This Is the Time To Consider Security Fully in Choosing the LNPA

As far as the record shows, the Commission has taken no comment on security requirements and has made no determination to waive the security assurances that are standard in similar contexts. In fact, it appears that the Commission has not yet considered security in the context of the LNPA choice. Nor has it sought the advice of the Executive Branch as its policies and past practice require.

The Commission may not defer to the NAPM and NANC on the question of which security measures are required for number portability or which candidate best meets those requirements. In the past, the Commission has deferred instead to the Executive Branch in setting security requirements for the telecommunications infrastructure. The Commission has recognized that “foreign participation in the U.S. telecommunications market may implicate significant national security or law enforcement issues uniquely within the expertise of the

organization involving malware installed by Chinese manufacturer on the hardware and software embedded in handheld scanners), <http://www.securityweek.com/hackers-attack-shipping-and-logistics-firms-using-malware-laden-handheld-scanners>.

³⁰⁸ See, e.g., Max Schleicher, *Re: You Recent Spear Phishing Attack*, TECHINSURANCE, June 13, 2014 (discussing how spear phishing attacks have become “more dangerous in recent years” as hackers improve their methods for using data from social media websites to customize emails to target their victims), <http://www.techinsurance.com/blog/cyber-liability/spear-phishing-study/>.

Executive Branch.”³⁰⁹ Acknowledging this unique Executive Branch expertise, the Commission has traditionally deferred to it when evaluating approvals and acquisitions of existing telecommunications infrastructure by foreign-owned companies.³¹⁰

There is no evidence that Congress intended the Commission to ignore the Executive Branch in the context of number portability. The Commission’s tradition of deference to the Executive Branch on security issues was already established when the 1996 Act gave the Commission authority over number portability. For example, in 1995, the Commission adopted “standards for regulating the entry of foreign carriers into the United States market for international telecommunications services.”³¹¹

³⁰⁹ Report and Order and Order on Reconsideration, *Rules and Policies on Foreign Participation in the U.S. Telecommunications Market: Market Entry and Regulation of Foreign-Affiliated Entities*, 12 FCC Rcd 23891, 23919, ¶ 62 (1997) (“*Foreign Participation Order*”).

³¹⁰ See, e.g., Public Notice, *Applications Granted for the Transfer of Control of STI Prepaid, LLC and STI Telecom Inc. to Angel Americas LLC*, WC Docket No. 13-242, DA 14-936 (FCC rel. June 27, 2014) (“Consistent with Commission precedent, the Bureaus accord the appropriate level of deference to the Executive Branch Agencies’ expertise on national security and law enforcement issues.”); Public Notice, *FCC Seeks Public Comment on Report on Process Reform*, 29 FCC Rcd 1338 (2014) (“The FCC seeks input from the Executive Branch and accords deference to the Executive Branch on” issues of “national security, foreign policy, law enforcement or trade policy concerns” in reviewing foreign ownership issues); Declaratory Ruling, *Commission Policies and Procedures Under Section 310(b)(4) of the Communications Act, Foreign Investment in Broadcast Licensees*, 28 FCC Rcd 16244, 16251, ¶ 14 (2013) (“Consistent with the Commission’s long-standing policy in reviewing foreign ownership of common carrier applicants and licensees, the Commission will continue to afford appropriate deference to the expertise of the Executive Branch agencies on issues related to national security, law enforcement, foreign policy, and trade policy.”).

³¹¹ Report and Order, *Market Entry and Regulation of Foreign-Affiliated Entities*, 11 FCC Rcd 3873, 3875, 3955-56, ¶¶ 1, 219 (1995) (“[I]n making our public interest determination, we will accord deference to the views of the Executive Branch on any national security, law enforcement, foreign policy, or trade policy concerns, or the interpretation of international agreements.”). While the Commission granted reconsideration of this Report in 1997, it “continue[d] to accord deference to the expertise of Executive Branch agencies in identifying and interpreting issues of concern related to national security, law enforcement, and foreign

The same approach should apply here. Now that the selection is in the hands of federal government decision-makers with access to national security expertise, a process should be established that allows a full consideration of security issues in making the selection. This process has two aspects. First, in some respects, security concerns can be addressed by adopting a set of security requirements, as is done by CFIUS, Team Telecom, FISMA, and other security-conscious federal regulatory and procurement programs. However, the two chief contenders, Neustar and Ericsson, do not present the same risk profile. They have different business models, as well as different technical and business practices. These have different security consequences. In addition to meeting a fixed minimum level, any future process established by the Commission should include security as a basis on which candidates compete. That is the only way to get the most security for the least cost, and the only way for the Commission and other agencies to be fully educated on the security risks and opportunities that each candidate offers.

The Commission should not be tempted to retrofit the existing competition – for example, by bolting a security agreement to the existing RFP. This approach would be defective and antithetical to the aims of this proceeding.

First, it would not fairly take into account the government's, and especially the Executive Branch's, interest in national security. Because its bid did not include any security costs, it is a near certainty that Ericsson will resist the acceptance of any security requirements that might add substantially to its costs and eat away at its profit margins. This approach turns security into an afterthought. Security should not be paid for with nickels found under the cushions of the administrator's couch.

policy that are relevant to an application pending before us.” *Foreign Participation Order*, 12 FCC Rcd at 23920, ¶ 63.

Further, it would not be fair to Neustar. Neustar would have no chance to demonstrate its superiority in terms of security. Making so significant a change without giving Neustar an opportunity to compete under the modified terms would be arbitrary, capricious, and not in accord with the government’s practice in analogous competitions. Government agencies “must treat all offerors equally, evaluating proposals evenhandedly against common requirements and evaluation criteria.”³¹² Similarly, agencies must consider all relevant factors in making their decisions.³¹³

Thus, under the FAR, the government must amend a solicitation when it changes the requirements or terms and conditions.³¹⁴ Courts have found that an agency’s failure to make these amendments can require resolicitation.³¹⁵ Accordingly, in the situation presented here, the Commission should give all candidates the chance to compete on any revised security criteria.

³¹² *J.C.N. Constr., Inc. v. United States*, 107 Fed. Cl. 503, 513, 514 (2012) (finding that lack of clarity in solicitation about the scope of work led to “uneven treatment” of offerors and was thus an “abuse of discretion”).

³¹³ *Great Lakes Dredge & Dock Co. v. United States*, 60 Fed. Cl. 350, 358, 366 (2004) (determining that decision to cancel solicitation was arbitrary and capricious where “the agency did not consider all relevant factors”); *Antarctic Support Assocs. v. United States*, 46 Fed. Cl. 145, 154-55 (2000) (stating that agency decision “will be set aside as arbitrary and capricious if the agency has not considered all relevant factors,” but that decision here was not because “the panel was aware of all relevant factors, reviewed them, and reached a decision based upon their scientific and technical expertise”); *cf. J.C.N. Constr.*, 107 Fed. Cl. at 510 (stating that agency’s procurement decision will lack a rational basis where “agency’s contracting officer ‘entirely failed to consider an important aspect of the problem’”) (citations omitted).

³¹⁴ 48 C.F.R. § 15.206.

³¹⁵ *Mangi Envtl. Grp., Inc. v. United States*, 47 Fed. Cl. 10, 18 (2000) (finding that agency’s procurement decision, which accepted bidder’s non-compliant proposal but failed to amend the solicitation to advise all offerors that “it decided to relax certain mandatory provisions,” thus “afford[ing] all offerors the opportunity to amend their proposals,” required amendment or resolicitation); *MVM, Inc. v. United States*, 46 Fed. Cl. 137, 143-44 (1999) (finding that public interest was served by requiring amendment and resolicitation where agency failed to amend solicitation as required by regulation); *cf. Beta Analytics Int’l, Inc. v. United States*, 44 Fed. Cl. 131, 139 (1999) (remanding for determination of prejudice where agency “should have afforded

In short, due to the significant national security issues that must be addressed in the selection of an LNPA and the current RFP's lack of provisions on security, the Commission must cure these deficiencies by adopting a set of security requirements and permitting all candidates to compete on all bases, including these additional security requirements.

CONCLUSION

For the foregoing reasons, the Commission should (1) declare that Ericsson's proposal does not qualify for consideration in light of its failure to satisfy the impartiality/neutrality requirements required by law and Commission precedent; (2) authorize the NAPM LLC to negotiate an extension to the current contract; and (3) issue a notice of proposed rulemaking to examine future arrangements for administration of the NPAC.

all offerors the opportunity to amend their proposals" but "declined to avail itself" of the amendment procedure, which would "have advised all offerors" of the change in requirements).

**SECOND CORRECTED COPY
REDACTED – FOR PUBLIC INSPECTION**

Respectfully submitted,

Brendan V. Sullivan, Jr.
David D. Aufhauser
Beth A. Stewart
WILLIAMS & CONNOLLY
725 12th Street, N.W.
Washington, D.C. 20005
202-434-5000

Stewart A. Baker
Kaitlin Cassel
STEPTOE & JOHNSON LLP
1330 Connecticut Avenue, NW
Washington, DC 20036
(202) 429-3000

Thomas J. Navin
Nancy J. Victory
Tyrone Brown
Brett Shumate
WILEY REIN LLP
1776 K Street, N.W.
Washington, D.C. 20006
(202) 719-7000

July 25, 2014

/s/ Aaron M. Panner
Aaron M. Panner
Evan T. Leo
Melanie L. Bostwick
KELLOGG, HUBER, HANSEN, TODD,
EVANS & FIGEL, P.L.L.C.
1615 M Street, N.W., Suite 400
Washington, D.C. 20036
(202) 326-7900

Leonard J. Kennedy
Scott M. Deutchman
J. Beckwith Burr
Richard L. Fruchterman, III
Aaron N. Goldberger
NEUSTAR, INC.
1775 Pennsylvania Avenue, N.W.
4th Floor
Washington, DC 20006
(202) 533-2705

Michele Farquhar
Praveen Goyal
Hogan Lovells US LLP
555 13th Street NW
Washington, DC 20004
(202) 637-5600

Counsel for Neustar, Inc.