

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

**HIGHLY CONFIDENTIAL AND RESTRICTED ACCESS  
CRITICAL INFRASTRUCTURE INFORMATION  
LETTER OF SUBMISSION OF NEUSTAR, INC.**

*Prepared by:*

Michael A. Sussmann  
PERKINS COIE, LLP  
700 Thirteenth Street, N.W.  
Washington, D.C. 20005  
(202) 654-6200

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

*On behalf of:*

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

November 6, 2014

November 6, 2014

Ms. Marlene H. Dortch  
Secretary  
Federal Communications Commission  
445 12th Street, S.W.  
Room TW-A325

*Electronically Filed*

Re: CC Docket No. 95-116; WC Docket No. 09-109

Dear Ms. Dortch:

We write on behalf of Neustar, Inc., to sum up and respond to the filings received by the Commission on the national security, law enforcement and public safety implications of choosing an NPAC vendor. In particular, we are responding to four filings by Ericsson's wholly owned subsidiary, Telcordia Technologies, Inc., d/b/a iconectiv ("Ericsson").<sup>1</sup>

## **I. Summary**

Ericsson has made four filings on national security issues since Neustar's most recent submission on the same topic. Ericsson's filings have simplified the issues before the Commission in several ways. First, Ericsson now accepts that the security concerns identified by Neustar are serious; second, it concedes the need to protect against compromise of the law enforcement platform; third, it recognizes that reusing LNPA code around the world is risky; and, fourth, it appears to accept that disruption of phone service in an emergency is also a legitimate security concern.<sup>2</sup>

Ericsson also concedes that each of these concerns must be mitigated by security measures: Personnel and network security for the law enforcement platform must be tight; code

---

<sup>1</sup> Ex Parte Response of Telcordia Technologies, Inc. D/B/A iconectiv to Neustar Reply Comments (Sept. 24, 2014) ("09-24-14 Ex Parte Response of Telcordia"); Ex Parte Response of Telcordia to Neustar Reply Comments, filed in the FCC Sensitive Compartmented Information Facility ("SCIF") (Sept. 24, 2014) ("SCIF Ex Parte Response of Telcordia"); Notice of Ex Parte by Telcordia Technologies, Inc. D/B/A/ iconectiv (Oct. 17, 2014) ("10-17-14 Ex Parte Response of Telcordia"); Notice of Ex Parte by Telcordia Technologies, Inc. D/B?A/ iconectiv (Oct. 27, 2014) ("10-27-14 Ex Parte Response of Telcordia"); *see also* Reply Comments of Telcordia Technologies, Inc., D/B/A/ iconectiv (Aug. 22, 2014) ("Ericsson Reply Comments").

<sup>2</sup> A fourth security concern identified by Neustar was that Ericsson's commitment to integrating number portability into the business and operational systems of telecommunications operators would make number portability a new vector for infection of every operator—a "one-stop shop" for critical infrastructure hackers. Ericsson has not addressed this risk, *see infra* note 33, which we take as a tacit concession that it is real as well.

Ms. Dortch  
November 6, 2014  
Page 3

should be written from scratch in the United States; and a host of other security measures should be adopted by the LNPA.

Ericsson further recognizes, as it must, that many of these necessary security measures are not specified in the RFP.

What remains in dispute is how these gaps can and will be filled. Ericsson says, in essence, that it will do anything the Commission wants as long as Neustar is not given a chance to compete on the same terms: It volunteers to use security measures that it says are part of its usual practice;<sup>3</sup> it argues that, properly understood, the RFP contains “robust” security provisions that “encompass” all necessary security measures;<sup>4</sup> and it points to **\*\*BEGIN HIGHLY CONFIDENTIAL INFORMATION\*\*** [REDACTED] **\*\*END HIGHLY CONFIDENTIAL INFORMATION\*\***

We disagree with Ericsson on this critical point. In our view, there is nothing “robust” about the security terms of the RFP. The report by The Chertoff Group, filed on September 30, 2014, highlights significant gaps in the RFP as compared to the applicable Framework for cybersecurity developed by the National Institute of Standards and Technology (“NIST”).<sup>6</sup> The Chertoff Group report shows that the RFP omitted entire categories of security requirements.<sup>7</sup> And the claim that the RFP encompasses all necessary security terms cannot be squared with the words of the RFP itself.<sup>8</sup> Several law enforcement priorities are not adequately addressed, if they are addressed at all, in the RFP documents. These include law enforcement approval of the LNPA’s personnel and security, protection of law enforcement queries, maintaining confidentiality of law enforcement data, prioritizing law enforcement access to the NPAC platform, maintaining LNPA supply chain standards, establishing an appropriate role for law enforcement in granting access to the NPAC, and protecting the integrity of NPAC code.

---

<sup>3</sup> Ericsson Reply Comments at 122-129; *see also* 09-24-14 Ex Parte Response of Telcordia at 12-13; SCIF Ex Parte Response of Telcordia.

<sup>4</sup> 09-24-14 Ex Parte Response of Telcordia at 4.

<sup>5</sup> Ericsson Reply Comments at 118.

<sup>6</sup> While the Framework is relatively recent, it is largely a restatement of standards that have long been recommended for comprehensive information security and that could easily have been incorporated into the RFP. *See, e.g.*, ISA-622443-2-1 (January 13, 2009); COBIT-5 (April 10, 2012); *see also* NIST, Framework for Improving Critical Infrastructure Cybersecurity 4, 20-35 (Feb. 12, 2014). These standards did exist when the RFP was released and could have been incorporated into its provisions.

<sup>7</sup> *See infra*, notes 11-24 and accompanying text.

<sup>8</sup> *See infra*, notes 34-64 and accompanying text.

Ms. Dortch  
November 6, 2014  
Page 4

Moreover, Ericsson egregiously misstates the risks associated with transition from Neustar’s LNPA Enhanced Analytics Platform (“LEAP”) to Ericsson’s Enhanced Law Enforcement Platform (“ELEP”) because Ericsson misunderstands the nature of the current LNP service. Ericsson assumes (erroneously) that LEAP is an LNP service and thereby covered by the LNP contract provisions relating to transition of services. However, LEAP is not an LNP service and—since the RFP contains no provisions relating to transition of the LEAP service—the RFP contains no requirements anywhere relating to transition from Neustar’s LEAP to Ericsson’s ELEP.

**\*\*BEGIN HIGHLY CONFIDENTIAL INFORMATION\*\*** [REDACTED]

**\*\*END HIGHLY CONFIDENTIAL INFORMATION\*\***

Thus, the principal remaining disagreement between the parties is how to cure the security deficiencies of the RFP. In Neustar’s view, the RFP simply omits a number of crucial security terms, it must be modified, and both parties must be given the chance to compete under the modified terms. Ericsson contends that the RFP can be construed in ways that would allow the Commission to avoid any further competition between Ericsson and Neustar.

Even on this issue there is some agreement. Both parties rely on the principles of federal procurement law as an important guide to deciding when the changes are so significant that they require that the government give all parties an opportunity to bid on the modified RFP. Applying these principles, Ericsson’s claim that security issues can be handled as matters of “contract administration” or vendor “responsibility” is belied by the significance of the RFP’s gaps. Proper security must be made part of the vendor evaluation process; it cannot be bolted on after a selection is made.

**II. Argument**

**A. The RFP’s Security Terms Are Not “Robust”—or Even Adequate**

The recent report by the Chertoff Group (“Chertoff Report”) highlights just how far from “robust” the RFP is. The Chertoff Report analyzes the RFP’s terms by comparing it to the NIST Cybersecurity Framework, which has been embraced by President Obama, Chairman Wheeler,

---

<sup>9</sup> See *infra*, notes 65-67 and accompanying text.

Ms. Dortch  
 November 6, 2014  
 Page 5

Members of Congress, leaders in the Executive Branch, telecommunications executives, and many others.<sup>10</sup> It finds major gaps “in both scope and specificity when compared with widely accepted national and international standards.”<sup>11</sup> Indeed, comparing the RFP’s terms to all 98 of the NIST framework’s subcategories, it finds that the RFP completely fails to address roughly 75% of the framework’s elements and only partially addresses another 15%.<sup>12</sup>

Many of the RFP’s omissions involve whole categories of security requirement. Among the remarkable gaps are items considered essential by the NIST framework and by security professionals generally:

1. **“Checklist security” v. “systemic security.”** Perhaps the biggest failing of the RFP is its “checklist” approach to security. As the Chertoff Report makes clear, security requires a systemic approach, one that begins with an inventory of network software and hardware and ends with a comprehensive plan for containing, responding to, and remediating an attack. The Report finds that the RFP lacks many of these crucial systemic requirements:
  - a. **Inventory and prioritization of assets not mentioned in RFP.** While acknowledging that data flows and access to data are covered by the RFP, the Report criticizes the RFP’s failure to require security that is grounded in an understanding of what’s on the network: *“However, inventory and prioritization*

---

<sup>10</sup> See Statement of Pres. Obama on the Release of the ‘Framework for Improving Critical Infrastructure Cybersecurity’ (Feb. 12, 2014), *available at* <http://www.gpo.gov/fdsys/pkg/DCPD-201400088/pdf/DCPD-201400088.pdf>; Tom Wheeler, Remarks at American Enterprise Institute (June 12, 2014), *available at* [http://transition.fcc.gov/Daily\\_Releases/Daily\\_Business/2014/db0612/DOC-327591A1.pdf](http://transition.fcc.gov/Daily_Releases/Daily_Business/2014/db0612/DOC-327591A1.pdf) (“The issuance of the Framework earlier this year has created a tremendous opportunity to make major, meaningful strides in cybersecurity. The Framework is a flexible, adaptable approach to risk management that can be applied by companies of all types and sizes across all sectors.”); Cybersecurity Framework for Improving Critical Infrastructure, What Others are Saying, *available at* [http://www.whitehouse.gov/sites/default/files/docs/cybersecurity\\_framework\\_-\\_what\\_others\\_are\\_saying\\_2\\_27.pdf](http://www.whitehouse.gov/sites/default/files/docs/cybersecurity_framework_-_what_others_are_saying_2_27.pdf) (citing support for NIST Framework from bipartisan group of Senators and Congressmen, as well as corporations including AT&T, Verizon, CenturyLink, Comcast Cable, Time Warner Cable, US Telecom, National Cable & Telecommunications Association); Testimony of Phyllis Schneck, Deputy Under Secretary for Cybersecurity, Department of Homeland Security, before the Senate Homeland Security and Governmental Affairs Committee (Mar. 26, 2014), *available at* <http://www.hsgac.senate.gov/download/?id=66d59b29-25ac-4dc1-a3af-040dcfe3bd38>.

<sup>11</sup> The Chertoff Group, *A Review of Security Requirements for Local Number Portability Administration* at 3 (Sept. 29, 2014) (“Chertoff Report”).

<sup>12</sup> *Id.* at 30-37, Appendix B.

Ms. Dortch  
 November 6, 2014  
 Page 6

*of assets, including personnel roles, are not identified as a requirement. While such inventory may be created and maintained in the course of system administration, they should be formally required and should become part of the criteria for pre-award and post-award evaluation of the vendor. . . . Maintaining an inventory of hardware and software assets—particularly for critical systems—is at the top of the CSC 20 list. These inventories form the foundation for ensuring that assets are securely configured—conversely, lack of inventories makes it impossible to ensure comprehensive configuration control. In addition, without valid asset inventory data, it may be impossible to achieve complete containment, response, and remediation following a security incident since remediation efforts will likely fail to account for all malicious activity hidden in non-inventoried assets.”<sup>13</sup>*

- b. Risk assessment not required by RFP.** The Report also found that the RFP said nothing about conducting “a complete risk assessment and risk management program to discover and monitor risks to the NPACs.”<sup>14</sup> An LNPA that does not conduct risk assessments has no basis for adjusting its security measures to meet evolving threats. As the Chertoff Report puts it, “A thorough risk assessment should occur at the beginning of the system development process and should inform security requirements, a principle embodied in NIST Special Publication 800-64, *Security Considerations in the System Development Lifecycle*.”<sup>15</sup>
- c. Life-cycle development not required by RFP.** The Report also notes that the RFP’s requirement of a life-cycle development methodology is nowhere extended to the LNPA’s security requirements: “*The FRS and TRD identify a requirement that software be developed using a lifecycle methodology, but neither document speaks to the need for information security to be formally factored into a system lifecycle management methodology to provide more holistic protection, including configuration control, data destruction, and continuous improvement. In the spirit of ‘an ounce of prevention is worth a pound of cure,’ integrating security planning into the system development lifecycle (‘SDLC’) early, e.g., at the requirements identification phase, can both (a) reduce the cost and complexity of building security into a system after the fact, and (b) align security and underlying business processes up front to make for a more seamless user experience.*”<sup>16</sup>

---

<sup>13</sup> *Id.* at 15-16 (emphasis in original).

<sup>14</sup> *Id.* at 3.

<sup>15</sup> *Id.* at 17 (emphasis in original).

<sup>16</sup> *Id.* (emphasis in original).

Ms. Dortch  
 November 6, 2014  
 Page 7

**d. No RFP requirement to update security and patch vulnerabilities.** Another critical gap in the RFP’s security requirements, as identified by the Chertoff Report, is the lack of a requirement for updating and maintaining security against current threats. The Report notes the omission of a provision for continuous assessment of threats and vulnerabilities and of processes for correctly testing, managing, and patching them: “[n]either the FRS nor the TRD contains any formal vulnerability scanning or patching requirements.”<sup>17</sup> To address the evolving threats that face the LNPA, the Report says, “security functionality must be continuously assessed for implementation, effectiveness, and impact through risk-monitoring capabilities. . . . Security is an ongoing challenge that requires constant, real-time monitoring of system conditions, including regular third-party red-teaming against constantly changing threat tactics.”<sup>18</sup>

**2. RFP void of personnel security requirements.** Similarly, the Report found that in general the solicitation documents “appear to contain no security-related personnel management provisions.”<sup>19</sup> This omission would be remarkable in any security document, but it is particularly so for a critical infrastructure service to be provided by a foreign-owned company. We would wager that every national security agreement with a foreign operator that is on file at the Commission sets rules for personnel security and for using U.S. nationals (and even cleared personnel) for particular functions.

These omissions are fundamental flaws; they are not, as Ericsson suggests, matters of unnecessary “detail” or “technical implementation.”<sup>20</sup> The authors of the Chertoff Report understand the difference. Whether discussing the creation of an asset inventory<sup>21</sup> or specific alert thresholds<sup>22</sup> or the formation of an incident response plan,<sup>23</sup> the Chertoff Report repeatedly emphasizes that not every detail must be spelled out, while at the same time insisting that “acquisition best practice dictates that [security requirements] be stated with specificity.”<sup>24</sup>

Nonetheless, Ericsson argues that federal procurement law somehow supports its assertion that these vital security concerns should be handled as matters of “contract

---

<sup>17</sup> *Id.* at 19 (emphasis in original).

<sup>18</sup> *Id.* at 21 (emphasis in original).

<sup>19</sup> *Id.* at 18 (emphasis in original).

<sup>20</sup> 09-24-14 Ex Parte Response of Telcordia at 2.

<sup>21</sup> Chertoff Report at 15.

<sup>22</sup> *Id.* at 20.

<sup>23</sup> *Id.* at 21-22.

<sup>24</sup> *Id.* at 23.

Ms. Dortch  
 November 6, 2014  
 Page 8

administration.”<sup>25</sup> This simply is not true. Rather, procurement regulations and case law require that detailed information security provisions be made part of solicitations well before contract award.

For example, during the acquisition planning phase, the Federal Acquisition Regulation (“FAR”) requires agency heads, before an RFP is even released, to “[e]nsure that . . . information technology acquisitions comply with . . . guidance and standards from the Department of Commerce’s National Institute of Standards and Technology.”<sup>26</sup> Moreover, the Department of Defense FAR Supplement (“DFARS”)—which governs approximately half of all Federal procurements by dollar value—requires that acquiring activities “shall ensure that all applicable Federal Information Processing Standards are incorporated *into solicitations*.”<sup>27</sup> When the DFARS refers to FIPS being incorporated in solicitations (i.e. RFPs), it means the federal standards incorporating the same NIST security controls that form the backbone of the NIST framework.<sup>28</sup> The Government Accountability Office (“GAO”)—which considers protests relating to contract formation, not administration—has upheld agencies requiring offerors to propose a technical approach that demonstrates compliance with detailed security criteria *prior to award*, and criticized agencies that give short shrift to detailed security requirements.<sup>29</sup>

Ignoring actual federal practice on security terms, Ericsson argues that bolting on a set of security obligations after selection is permissible under government procurement law. But even

---

<sup>25</sup> 09-24-14 Ex Parte Response of Telcordia at 18-19.

<sup>26</sup> FAR (48 C.F.R. §) 7.103(w).

<sup>27</sup> DFARS (48 C.F.R. §) 239.7201 (emphasis added).

<sup>28</sup> *See, e.g.*, NAT’L INST. OF STANDARDS & TECH., FIPS PUBLICATION 200, MINIMUM SECURITY REQUIREMENTS FOR FEDERAL INFORMATION AND INFORMATION SYSTEMS v (2006) (citing NIST SP 800-53 as the security controls required for federal information systems); NAT’L INST. OF STANDARDS & TECH., FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY 35 (2014) (identifying NIST SP 800-53 as a core security standard for the NIST framework); Chertoff Report at 9, 18, 27 (identifying NIST SP 800-53 as necessary to securing the NAPM and LNPA).

<sup>29</sup> For decisions upholding detailed security requirements in solicitations and evaluations, *see AIS Eng’g Inc.*, B-406186, 2012 CPD ¶ 106 at 6 (agency properly excluded offeror from further consideration for award where offeror failed to adequately detail approach to network security); *Operational Resource Consultants, Inc.*, B-299131.1 et al., 2007 CPD ¶ 38 at 10 (agency properly downgraded the protester’s proposal because it failed to demonstrate experience in compliance with FISMA and ISO:27001—a standard mentioned in the Chertoff Report). Compare these decisions with the result in *Pricewaterhouse Coopers LLP*, where the agency improperly overlooked the protester’s significant strength in its FISMA expertise and instead myopically focused on the awardee’s lower price and supposed past performance advantage. B-409537 et al., June 4, 2014, 2014 WL 4384605, at \*9.

Ms. Dortch  
 November 6, 2014  
 Page 9

the cases that Ericsson cites make clear that the government may not allow material changes either to the solicitation or to one candidate’s proposal, without giving equal opportunity to all bidders.<sup>30</sup> In fact, Ericsson itself recognizes that the courts and GAO determine materiality by considering “factors such as ‘the extent of any changes in the type of work, period of performance and costs.’”<sup>31</sup> Where Ericsson’s argument fails is in its claim that, “[h]ere there is no material change to the nature, scope, duration, or volume of work.”<sup>32</sup> It is plain that curing the security gaps identified by law enforcement and the Chertoff Report will touch all aspects of the solicitation and of the candidates’ proposals and will demand significant change in the nature, scope, and costs of the LNPA’s activities. For example, Ericsson’s new offer to develop necessary code “from scratch,” when its proposal made no mention of the risks that come with new code, fundamentally changes the nature of its proposal.

**B. Law Enforcement’s Missing Requirements Cannot be Shoehorned Into the RFP**

Ericsson’s claim that the RFP encompasses all necessary security terms cannot be squared with the federal procurement principle that security requirements should be specified.<sup>33</sup>

---

<sup>30</sup> See 09-24-14 Ex Parte Response of Telcordia at 16-18; see also Neustar Reply Comments at 70-76.

<sup>31</sup> 09-24-14 Ex Parte Response of Telcordia at 17.

<sup>32</sup> 09-24-14 Ex Parte Response of Telcordia at 18.

<sup>33</sup> While Ericsson has largely conceded the importance of three security risks identified in Neustar’s past filings by declaring that it intends to fix them, it simply fails to respond to the fourth, which flows from Ericsson’s strong interest in providing many outsourced technology services to U.S. telecommunications operators. Neustar Comments at 102-107. In keeping with its strategy of encouraging technological dependence on the part of operators, Neustar argued, Ericsson has promoted deeper integration of number portability services into operators’ business and operational systems. After noting that this strategy raises neutrality issues, Neustar laid out the security implications: **\*\*BEGIN RESTRICTED - CRITICAL INFRASTRUCTURE INFORMATION\*\***

**\*\*END RESTRICTED - CRITICAL INFRASTRUCTURE INFORMATION\*\***

Faced with this serious security concern and apparently lacking a serious answer, Ericsson ignores the plain words of Neustar’s filing and pretends that Neustar’s security concern is a neutrality argument, responding that **\*\*BEGIN RESTRICTED - CRITICAL INFRASTRUCTURE INFORMATION\*\***

**\*\*END RESTRICTED - CRITICAL INFRASTRUCTURE INFORMATION\*\***

Ms. Dortch  
 November 6, 2014  
 Page 10

Taken at its broadest (and as we will see, that is how Ericsson takes it), Ericsson’s line of argument would permit the NAPM’s RFP simply to require “all appropriate security measures,” leaving the entire suite of security obligations to be negotiated separately and after the fact.<sup>34</sup> That course of action would be inconsistent with the NIST Cyber Security Framework, which has been widely adopted precisely so that it can be used to describe security requirements more specifically and enforceably. Given the stakes for the country, it would be foolish to reject the framework and rely instead on abstract and unenforceable security requirements.

In any event, Ericsson’s reading of the RFP goes well beyond abstract and unenforceable. To find law enforcement’s requirements in the RFP—both with regard to LNP administration generally, and provision of the LEAP service specifically—Ericsson tortures the document beyond recognition.<sup>35</sup>

### **LNP Administration**

- 1. No law enforcement approval of LNPA personnel and security is required.** For example, Ericsson argues that several law enforcement priorities, such as the requirements that LNPA personnel be cleared and that a written security plan be prepared in consultation with law enforcement, can be found in an RFP provision that requires each law enforcement agency to enter into a contract with the LNPA before it can have access to the law enforcement platform.<sup>36</sup> However, this provision has nothing to do with

---

Ericsson’s reply simply misses the point. Integration is, after all, the vision that Ericsson has been touting to the world. But with that new capability comes new risks to the entire telecommunications infrastructure. How does Ericsson propose to mitigate those risks? It doesn’t.

<sup>34</sup> Ericsson’s argument that in federal procurements security requirements relate solely to an offeror’s responsibility and not its technical merit is not only factually inaccurate, it is legally incorrect as well. 09-24-14 Ex Parte Response of Telcordia at 19-20; Ericsson Reply Comments at 121-122 & n.365. As shown above, the FAR, DFARS, and case law demonstrate that detailed security criteria are frequently included—and many times required to be included—in Federal solicitations. *See supra* notes 26-29 and accompanying text. Moreover, where a solicitation specifically provides for traditional responsibility concerns as an evaluation factor or criteria, an agency can and should require offerors to demonstrate detailed compliance with those criteria. *See* Nomura Enters., Inc., B-277768, 97-2 CPD ¶ 148; Continental Maritime of San Diego, Inc., B-249858 et al., 93-1 CPD ¶ 230 at 4-5.

<sup>35</sup> Ericsson attributes the list of law enforcement requirements to Neustar, but the list is in fact derived from the comments of law enforcement agencies. *See* Reply Comments of Neustar at 65-66 (citing Reply Comments of the Federal Bureau of Investigation, the Drug Enforcement Administration, the United States Secret Service, and the U.S. Immigration and Customs Enforcement).

<sup>36</sup> 09-24-14 Ex Parte Response of Telcordia at 8-9.

Ms. Dortch  
 November 6, 2014  
 Page 11

law enforcement imposing requirements on the LNPA. The clear purpose of the provision is to impose requirements on law enforcement agencies by denying them access to the platform if they do not meet the conditions set by the NAPM LLC. Each agreement is between the LNPA and a single agency;<sup>37</sup> law enforcement agencies do not generally negotiate contracts as a group. What’s more, the LNPA will be audited to make sure that it is charging law enforcement agencies for their use of the platform and that it is preventing the law enforcement platform from interacting with the production NPAC/SMS.<sup>38</sup> These and other provisions of the RFP make plain that law enforcement agencies are not the ones meant to have bargaining power in the negotiation of the agreements. There is not the slightest indication of intent on the part of the NAPM to allow law enforcement agencies to negotiate additional security provisions, either for the law enforcement platform or for the NPAC system as a whole. The NAPM instead designed the RFP to *impose* limits on law enforcement. It was intended to ensure that, if law enforcement wanted access to LEAP, it would abide by NAPM’s rules, it would pay its own way,<sup>39</sup> its platform would not interfere with number portability services,<sup>40</sup> and the type and use of data it received from the platform would be strictly limited.<sup>41</sup>

2. **No government scrutiny of LNPA supply chain is required.** Further, in response to the requirement that there be a detailed accounting of supply chain standards and procedures specific to the query system, Ericsson points to one section of the FRS, §

---

<sup>37</sup> 2015 LNPA RFP § 11.2, Req. 5 (“The Enhanced Law Enforcement Platform *Service shall only be provided* to a Qualified Recipient *if such party enters* into and executes the Enhanced Law Enforcement Platform Service Agreement that satisfies the requirements set forth in the Master Agreements and that is in substantially the form approved by the NAPM LLC. . . .”) (emphasis added).

<sup>38</sup> 2015 LNPA RFP § 11.2, Req. 16.

<sup>39</sup> 2015 LNPA RFP § 11.2, Req. 4 (“[N]o charges or costs associated with the Enhanced Law Enforcement Platform Service help desk shall be included in any charges to NPAC/SMS Users. . . .”); Req. 18 (The LNPA . . . shall look solely to the respective Qualified Recipients for any and all compensation for the provision of the Enhanced Law Enforcement Platform Service. . . .”).

<sup>40</sup> 2015 LNPA RFP § 11.2, Req. 3 (“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 Enhanced Law Enforcement Platform Service.”); Req. 18 (“The LNPA must agree and acknowledge that the Enhanced Law Enforcement Platform Service is discretionary and elective . . . and is not necessary for the provision of number portability.”).

<sup>41</sup> 2015 LNPA RFP § 11.2, Req. 9 (“Enhanced Law Enforcement Platform services shall not provide Qualified Recipients, either directly or indirectly, access to the NPAC/SMS or any NPAC User Data other than the Enhanced Law Enforcement Platform Data Elements. . . whether or not such data elements or information is obtained from public sources or any other source.”).

Ms. Dortch  
 November 6, 2014  
 Page 12

7.8.<sup>42</sup> FRS § 7.8 requires that “NPAC SMS shall be developed using a corporate policy governing the development of software,” and provides for certain access controls for maintenance, support, and operations. While it is good to know that the vendor will follow “corporate policy” in development, this does nothing to ensure accounting of supply chain standards and procedures—and it is not at all specific to the query system. Further, the law enforcement requirement to which Ericsson appears to be replying was particularly concerned with ensuring Government checks on the supply chain, such that this supply chain accounting would be provided to the Commission with the Commission empowered to request related mitigation steps.<sup>43</sup> It is more than a stretch to say that these protections are encompassed in a requirement to follow “corporate policy.”

3. **No government role in granting access to NPAC.** Additionally, federal law enforcement agencies seek a role in ensuring that only suitable persons have access to the NPAC system; Ericsson argues that this requirement is encompassed by provisions such as FRS §§ 7.4.1, 7.4.2 and RFP § 5.1.<sup>44</sup> While these sections do specifically delineate other parties’ roles in this process, they say nothing about a role for law enforcement. In fact, they seem quite clearly to exclude such a role. For example, FRS § 7.4.1, Req. 7-49.1 states, “NPAC SMS *shall only allow the NPAC Security Administrator* to authorize users” (emphasis added). Similarly, FRS § 7.4.2, Req. 7-60 states, “NPAC SMS shall allow *only NPAC personnel* to modify access rights to a resource” (emphasis added). RFP § 5.1 is even more detailed in its description of the process for new user evaluation and approval. It provides a role for the NAPM LLC when the LNPA cannot determine if the applicant is a Service Provider or PTRS and a role for an “independent third party evaluator” where the applicant is a PTRS or is an existing user that has received a

---

<sup>42</sup> 09-24-14 Ex Parte Response of Telcordia at 10. As an example of the importance of evaluating supply chain risk before award, the Department of Defense requires contracting officers to consider including supply chain risk as an evaluation factor in solicitations for information technology procurements. DFARS 215.304(c)(v).

<sup>43</sup> Reply Comments of the Federal Bureau of Investigation, the Drug Enforcement Administration, the United States Secret Service, and the U.S. Immigration and Customs Enforcement at 6.

<sup>44</sup> 09-24-14 Ex Parte Response of Telcordia at 8-9. Ericsson also cites several requirements in RFP § 11.2, including Req. 1, Req. 2, Req. 11, Req. 12, Req. 14, Req. 15, and Req. 16. These requirements provide that LEAP services can only be provided to Qualified Users (law enforcement agencies and PSAPs), discuss limits on use of service provider information, require Qualified Users to comply with applicable laws, require annual re-verification for Qualified Users, require an annual report listing all Qualified Users, and call for an audit of LEAP service for compliance with certain specified requirements. They do not discuss requiring the LNPA to coordinate with law enforcement regarding the suitability of persons with access to the LNP system.

Ms. Dortch  
November 6, 2014  
Page 13

“Misuse Allegation.”<sup>45</sup> Yet, none of these provisions even suggest a review by federal law enforcement agencies for security purposes.

- 4. No requirement regarding origin of LNPA code.** Perhaps even more significant, Ericsson does not even try to argue that its promise to write code for the LNPA “from scratch in America” is encompassed by the RFP. Nor does it claim that its RFP response included a promise to write the code “from scratch in America.” Instead, it makes a much narrower claim – that it always intended to write the code from scratch.<sup>46</sup>

**\*\*BEGIN HIGHLY CONFIDENTIAL INFORMATION\*\*** [REDACTED]

[REDACTED]

**\*\*END HIGHLY CONFIDENTIAL INFORMATION\*\*** Nor did that fragment of a sentence alert the NAPM to the transition risk associated with Ericsson’s current plan to write new code from scratch. New code means new bugs and other vulnerabilities, and the NAPM deserved a better opportunity to consider the risk created by writing new code when it evaluated Ericsson’s bid for performance, reliability, and transition risk. Instead, Ericsson made its offer to

---

<sup>45</sup> 2015 LNPA RFP § 5.1.

<sup>46</sup> In its most recent filing, Ericsson similarly argues that Neustar has pointed to security risks both in re-using code and in using new code and that it “cannot have it both ways.” 10-27-14 Ex Parte Response of Telcordia at 5. This assertion misunderstands the security concerns. A new LNPA will bring inherent security risks, whether it uses old code or new code. Neustar has simply shown that, whether the code Ericsson uses is old or new, there are unaddressed security risks regarding its plan for code development that must be considered.

<sup>47</sup> LNPA Procurement Presentation and Q&A in Denver, Colorado: Telcordia Technologies, Inc., Transcript at 169:12-14 (Aug. 6, 2013) (“Telcordia Transcript”).

Ms. Dortch  
November 6, 2014  
Page 14

write code from scratch only after the NANC recommendation was made and the security issues with their proposal became apparent.<sup>48</sup>

**LEAP and Public Safety Queries**

- 1. No requirement to protect law enforcement queries from surveillance.** Ericsson claims that one of law enforcement’s most important requirements—a bar on tracking, logging, and storing law enforcement queries—is encompassed within the RFP.<sup>49</sup> This prohibition, however, is not just missing from the RFP; it is directly inconsistent with Ericsson’s RFP response<sup>50</sup> and, as Ericsson makes clear in their most recent filing, with the RFP itself.<sup>51</sup>

---

<sup>48</sup> If anything, the details of Ericsson’s oral presentation revive the security concerns that its offer to write code from scratch tries to put to rest. In describing on August 6 what it planned to borrow from its existing deployments, Ericsson’s representative said, **\*\*BEGIN HIGHLY CONFIDENTIAL INFORMATION\*\*** [REDACTED]

[REDACTED]

**\*\*END HIGHLY CONFIDENTIAL INFORMATION\*\***

<sup>49</sup> 09-24-14 Ex Parte Response of Telcordia at 8. Ericsson cites two RFP provisions: RFP § 11.2, Req. 2, which states that the LEAP service shall only be provided to law enforcement agencies and PSAPs, and RFP § 11.2, Req. 5, which as discussed above requires a law enforcement agency to enter into a contract with the LNPA before it can have access to the LEAP system. Neither of these requirements touches on obligations of the LNPA in how it handles queries.

<sup>50</sup> We have pointed out already that Ericsson has badly misrepresented its RFP response on this question. See Neustar Ex Parte Response at 8 (Sept. 23, 2014); Neustar Reply Comments at 66-67.

<sup>51</sup> 10-27-14 Ex Parte Response of Telcordia at 2, 5-6.

Ms. Dortch  
 November 6, 2014  
 Page 15

In its advocacy, as we have already pointed out, Ericsson has tried to muddle the difference between the two systems that the RFP requires for law enforcement investigating a crime. But the difference is straightforward. Large agencies with a high volume of investigations are likely to use the ELEP, which offers online access to many telephone numbers. For agencies with fewer numbers to process, the RFP calls for a simpler Interactive Voice Response (“IVR”) system that can provide information about twenty numbers at a time. Law enforcement can use either system to obtain information during an investigation, and the security concerns do not differ from one system to the other. This is how Ericsson understood the two systems when it responded to the RFP.<sup>52</sup> Its response explicitly **\*\*BEGIN HIGHLY CONFIDENTIAL INFORMATION\*\***

[REDACTED]

[REDACTED]

[REDACTED] **\*\*END**

**HIGHLY CONFIDENTIAL INFORMATION\*\***

Because the two systems serve the same purpose and raise the same security issues, any concern about the recording of law enforcement queries is likely to apply with equal force to both systems. Unfortunately, despite law enforcement security concerns about the recording of queries, the RFP expressly requires that the IVR system be able to record law enforcement queries, and it is silent about whether the ELEP must be able to record such queries. Not surprisingly, Ericsson promised that it would be able to record IVR queries. In fact, in order to be responsive to the RFP, any bidder had to offer this capability.

This fact, however, is not an answer to the security concern regarding recording of queries; it is instead proof that the RFP, drafted without law enforcement input, did not adequately take security into account and even directly contradicts the security concerns that have been raised by law enforcement. When Ericsson attempts to explain its response by pointing to the RFP requirement to track and log IVR queries,<sup>55</sup> it only emphasizes the failure of the RFP itself to protect law enforcement’s interests. By

---

<sup>52</sup> Even Ericsson’s most recent Ex Parte recognizes the application of the IVR system to law enforcement queries. Ericsson states that “[t]he RFP required each bidder to verify that it would provide an IVR that could be accessed by . . . law enforcement agencies.” 10-27-14 Ex Parte Response of Telcordia at 5. It is unclear how Ericsson squares this statement with its assertion a few lines later that “Telcordia will not track, monitor, or maintain records of law enforcement queries.” *Id.* at 6. Ericsson clearly recognizes that law enforcement agencies would use IVR and that the RFP requires certain records regarding numbers queried.

<sup>53</sup> See TRD Detailed Response § 7.7 at Telcordia08112.

<sup>54</sup> See TRD Detailed Response §7.8 at Telcordia08112.

<sup>55</sup> See 10-27-14 Ex Parte Response of Telcordia at 2, 5-6.

Ms. Dortch  
 November 6, 2014  
 Page 16

requiring the LNPA to keep records that explicitly include “the telephone numbers inquired about” and the “results of the inquiry(ies),”<sup>56</sup> the RFP mandates a policy that contradicts law enforcement’s security requirements and exposes law enforcement information to compromise. Significantly, while Ericsson continues to state that it will not record ELEP queries, it will not (and cannot) commit that it will not provide recording capabilities for law enforcement queries made through IVR. To do so would be to admit that the current RFP calls for the exact opposite of what security and law enforcement needs.

In any event, Ericsson’s current promise—it will not record law enforcement queries made through ELEP, but it will continue to record law enforcement queries made through the IVR as required by the RFP—does not get to the heart of law enforcement concerns and leaves many law enforcement agencies facing a security risk that could compromise sensitive investigations. In order to fully address the security risk and ensure that *all* queries remain confidential, no matter which system law enforcement uses, change to the RFP is required.

2. **Confidentiality of law enforcement queries not required.** Ericsson says that several sections of the RFP and FRS support a requirement that LEAP queries remain confidential and that the LNPA vendor cannot have unwarranted visibility into the queries submitted.<sup>57</sup> The requirements to which Ericsson points, however, have nothing to do with restricting the LNPA and everything to do with restricting law enforcement. They provide that only qualified law enforcement agencies have access to the platform.<sup>58</sup> And they protect only the confidentiality of any *service provider* information that may be given to law enforcement in response to queries, while remaining entirely silent on the confidentiality of law enforcement’s investigative targets.<sup>59</sup> Far from encompassing law enforcement’s requirements, the RFP deliberately excludes them.
  
3. **Failure to prioritize the law enforcement platform.** In response to the FBI’s request that repairs and restoration of the LEAP system be prioritized if it fails in whole or in part, Ericsson points to three separate sections discussing basic service level protections for the entire LNPA system.<sup>60</sup> While these are important provisions to ensure continuity of LNPA services generally, they make no reference to LEAP and therefore do nothing to prioritize repairing and restoring LEAP functionality. Instead, (lack of) prioritization of LEAP is covered more clearly and directly in a separate provision, which explicitly

---

<sup>56</sup> 2015 LNPA RFP § 6.9, Req. 10.

<sup>57</sup> 09-24-14 Ex Parte Response of Telcordia at 7-8.

<sup>58</sup> See 2015 LNPA RFP § 11.2, Req. 8; FRS § 7.4.1.

<sup>59</sup> See 2015 LNPA RFP § 11.2, Req. 13.

<sup>60</sup> 09-24-14 Ex Parte Response of Telcordia at 9.

Ms. Dortch  
 November 6, 2014  
 Page 17

instructs that maintenance of the law enforcement platform is to be the lowest priority in relation to other LNPA services (“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 Enhanced Law Enforcement Platform Service.”).<sup>61</sup>

- 4. Failure to provide for LEAP transition.** Ericsson also misreads the relevant contracts in order to downplay the risks of making a transition from Neustar’s LEAP to Ericsson’s ELEP. Ericsson implies (erroneously) that LEAP is an LNP service and thereby covered by the LNP contract provisions relating to transition of services. However, LEAP is not an LNP service and—since the RFP contained no provisions relating to transition of the LEAP service—*there are no requirements anywhere relating to transition from Neustar’s LEAP to Ericsson’s ELEP.* That presents significant risk for the FBI and the other law enforcement and public safety agencies that have come to rely on LEAP. Notwithstanding, Ericsson offers the bland assurance that the transition from Neustar’s LEAP to Ericsson’s ELEP poses no transition risk because **\*\*BEGIN RESTRICTED - CRITICAL INFRASTRUCTURE INFORMATION\*\***

**\*\*END RESTRICTED - CRITICAL**

**INFRASTRUCTURE INFORMATION\*\*** But this assurance is at odds with the nature of LEAP with respect to the LNP services.

A technical and contractual prerequisite to the provisioning of LEAP services is that the provider of LEAP must also be the LNPA and—consistent with that requirement—the RFP requires the new LNPA to also provide LEAP. No one other than the LNPA can be expected to provide such services; only the LNPA is in a position to stand behind the data that LEAP and ELEP will be providing to public safety officials. Unfortunately, the current LNPA contracts simply do not provide specifics concerning how and when LEAP will be provided by the new LNPA.<sup>62</sup> Thus, for practical reasons, Ericsson must be in a position to offer ELEP services at the time it commences LNP services; no time for concurrent provision of service is contemplated in the RFP. Avoiding an interruption in service and maintaining high service levels for law enforcement will require comprehensive testing prior to launch of the service, something that should be properly detailed in a revised RFP. The RFP’s failure to specify required LEAP functionality and service levels, and to provide adequately for service transition, can and should be cured in the same RFP round that is needed in order to address *all* security issues.

---

<sup>61</sup> 2015 LNPA RFP § 11.2, Req. 3 (emphasis added).

<sup>62</sup> For example, the RFP is silent regarding how the new LNPA will be held accountable in the provision of the services. In addition, there are no testing or certification requirements in the RFP that the law enforcement community can rely on to ensure that the service being offered by the new LNPA will meet existing service levels or quality.

Ms. Dortch  
November 6, 2014  
Page 18

- 5. Failure to provide for 9-1-1 database transition for public safety and emergency responders.**<sup>63</sup> Ericsson makes the same error when it provides assurances about the functioning during a transition of the 9-1-1 Automatic Location Identification (ALI) database. This database is used to locate callers making 9-1-1 calls. It must be modified whenever a number is ported because only the current carrier has up-to-date address information. Any errors in this service could prevent delivery of a 9-1-1 call to the proper PSAP, potentially leading to loss of life or property. Timely and rapid correction of the ALI data by comparing it with NPAC data is a process separate from the LEAP and number porting process and is often undertaken by the 9-1-1 service provider. Presently, information for this service is provided by Neustar as an ancillary service to the NPAC and the 9-1-1 community has rightly raised concerns as to whether this information will still be available during a transition and ultimately by a new vendor. Because this service is dependent upon NPAC information, this matter must be addressed in a revised RFP.

As these examples demonstrate, the RFP's requirements are not robust security provisions. Nor are law enforcement's security requirements mere details encompassed by the RFP. That document covers far less important matters in far more detail; it mandates the speed by which live operators must answer Help Desk calls down to the second.<sup>64</sup> The RFP's omission of law enforcement requirements was not a matter of leaving the details to later administration; they are left out because they are not required by the current document. The RFP should be modified to take into account the security concerns of the Executive Branch, and both participants in the competition should be permitted to respond to the modified RFP.

**\*\*BEGIN HIGHLY CONFIDENTIAL INFORMATION\*\***

■ [REDACTED]

---

<sup>63</sup> Ericsson goes out of its way in its most recent filing to clarify that it is not responsible for “undisclosed ancillary services” that are not in the RFP. 10-27-14 Ex Parte Response of Telcordia. This likely includes provision of services such as the 9-1-1 ALI database and only further underlines the security concerns, not only about Ericsson's ability to provide this service, but about the inadequacies of the RFP itself.

<sup>64</sup> See 2015 LNPA RFP § 9.15, Req. 12 (“Minimum 90% calls during Normal Business Hours answered by live operators within 10 seconds.”); see also, e.g., 2014 LNPA FRS § 7.4.1, Req. 7-32.2 (requiring the default time period for “Non-use Disconnect tunable parameter” be set at “60 minutes”); FRS § 7.4.1, Req. 7-33.2 (requiring the default number of allowable incorrect login attempts be set at 3); FRS § 7.4.1, Req. 7-47.2 (mandating the exact language required in the “pre-login advisory warning message”).

Ms. Dortch  
November 6, 2014  
Page 19

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] **\*\*END HIGHLY CONFIDENTIAL INFORMATION\*\***

Pursuant to Section 1.1206 of the Commission’s rules, 47 C.F.R. § 1.1206, a copy of this letter is being filed via ECFS. If you have any questions, please do not hesitate to contact us.

<sup>65</sup> Ericsson Reply Comments at 118.

<sup>66</sup> Executive Order 13456 sec. 7(a) (Jan. 23, 2008) (“The Committee, or any lead agency acting on behalf of the Committee, may seek to mitigate any national security risk posed by a transaction that is not adequately addressed by other provisions of law by entering into a mitigation agreement with the parties to a transaction or by imposing conditions on such parties.” (emphasis added)).

<sup>67</sup> *Id.* at 123.

Ms. Dortch  
November 6, 2014  
Page 20

Sincerely,

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

Michael A. Sussmann  
PERKINS COIE, LLP  
700 Thirteenth Street, N.W.  
Washington, D.C. 20005  
(202) 654-6200

cc: Daniel Alvarez  
Nicholas Degani  
Rebekah Goodheart  
David Goldman  
Amy Bender  
Julie Veach  
Jonathan Sallet  
Kris Monteith  
David Simpson  
Roger Sherman  
Lisa Gelb  
Michele Ellison  
Randy Clarke  
Ann Stevens  
Sanford Williams  
Diane Griffin Holland  
Neil Dellar