

REDACTED—FOR PUBLIC INSPECTION

October 17, 2014

Ex Parte

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

Re: *Telephone Number Portability, et al.*, CC Docket No. 95-116, WC Docket Nos. 07-149 & 09-109

Dear Ms. Dortch:

On October 15, 2014, Richard Jacowleff, Chris Drake and Joel Zamlong of Telcordia Technologies, Inc., d/b/a iconectiv (“Telcordia”), Rear Admiral Jamie Barnett (USN, ret.) and Courtney Sullivan of Venable LLP, Jason Carey of McKenna, Long & Aldridge, LLP, John MacGaffin, a consultant with Deloitte & Touche LLP, Edward Stroz of Stroz Friedberg, and I, all on behalf of Telcordia, met with Rear Admiral David Simpson (USN, ret.), Lisa Gelb, Ken Moran, Ken Burnley, Nick Bourne, Randy Clarke, Diane Griffin Holland, Greg Intoccia, Allan Manuel, Ann Stevens, Jane Kelly, Sanford Williams, all of the FCC staff, regarding the pending selection of a Local Number Portability Administrator. This letter summarizes Telcordia’s presentation.

Telcordia has extensive experience both with U.S. number portability through its carrier gateway products and with operating other sensitive U.S. telecommunications routing and rating databases, such as the LERG and BIRRDS, as previously set forth in Telcordia’s Comments.¹ Telcordia has substantial experience with U.S. number portability, and has been an active participant in U.S. number portability since its inception.

Telcordia is taking substantial steps to protect the security of the Number Portability Administration Center (“NPAC”) database that it is building. Contrary to Neustar’s claims, Telcordia is not reusing foreign code for its U.S. NPAC and never stated it would do so. Telcordia is building the U.S. database with new code, reflecting that unique state of the U.S. telecommunications industry and its local number portability processes. In doing so, Telcordia is

¹ Comments of Telcordia Technologies, Inc., WC Docket No. 07-149 & 09-109 and CC Docket No. 95-116, at 6-8 (filed July 25, 2014)

being attentive to supply chain management. Among other things, it is not outsourcing code development to non-U.S. sources. ****BEGIN HIGHLY CONFIDENTIAL**** [REDACTED]

[REDACTED]

****END HIGHLY CONFIDENTIAL**** What is more, Telcordia's use of Sungard AS to provision datacenter hardware and software will provide robust security and service continuity protection. Telcordia's NPAC will benefit from Sungard's substantial experience in protecting the databases that it hosts from attacks, as well as the capabilities Sungard brings for network monitoring and service restoral. This is a substantial advantage from a security and service continuity perspective over a self-provisioned solution.

As Telcordia operates the NPAC, the NIST Cybersecurity Framework will provide key organizing principles. ****BEGIN HIGHLY CONFIDENTIAL**** [REDACTED]

[REDACTED]

****END HIGHLY CONFIDENTIAL****

Telcordia will also take care to ensure a secure operating environment for the Enhanced Law Enforcement Platform ("ELEP") required to be provided by the RFP. The ELEP is a copy of the NPAC database downloaded to a separate LSMS server for the exclusive use of law enforcement. Telcordia will not monitor these queries—and has never stated otherwise. Per the terms of the RFP, the ELEP will be limited to the data elements specified by the RFP, and will have controlled, restricted access. In the absence of a license to use existing ELEP software, Telcordia will be building the ELEP to the law enforcement agencies' interface specifications, ****BEGIN RESTRICTED ACCESS – CRITICAL INFRASTRUCTURE**

INFORMATION** [REDACTED] ****END RESTRICTED ACCESS – CRITICAL INFRASTRUCTURE INFORMATION**** As with the NPAC, Telcordia will be developing its own code for the ELEP; however, that development time should not delay overall NPAC testing an implementation as they can occur concurrently.

With respect to the transition for both the main NPAC and the ELEP, Telcordia anticipates working with industry and law enforcement, respectively, to develop the testing plan. As required by the procurement documents, Telcordia will be building an NPAC that is compatible with all existing interface specifications. It will work with the industry to develop and implement a comprehensive test plan to ensure that all constituents can process porting transactions, ****BEGIN RESTRICTED ACCESS – CRITICAL INFRASTRUCTURE INFORMATION**** [REDACTED] ****END RESTRICTED ACCESS – CRITICAL INFRASTRUCTURE INFORMATION**** Smaller providers that use the web-based GUI may need to be familiarized with a slightly different screen layout, but the fields are specified and thus must be the same. Thus, for the vast majority of carriers, transition costs will be minimal. A small subset of larger carriers and service bureaus will likely undertake more extensive testing of direct connections with the NPAC, and those would incur somewhat higher costs. The S²ERC Study projected those costs for larger carriers, based on a comparison with the implementation of the number pooling NPAC release, to “top out at a little under \$600,000.”²

We noted that the procurement documents appropriately addressed security in broad terms, with specifics to be worked out further in contract implementation. This is consistent with how security generally is handled in government procurements—including sensitive national security procurements. By framing the RFP and other procurement documents in general terms, the specifics of security implementation can evolve quickly without going outside the scope of the original procurement. This is particularly the case here, because security, as well as other enhancements such as the IP Transition, were specifically included within the scope of the existing bids. Put differently, to the extent that necessary security measures turn out to be more rigorous and costly than Telcordia projected when it submitted its bid, the business risk lies with Telcordia. Telcordia cannot, in that situation, seek a price modification from NAPM.

Telcordia understands that, if selected as the LNPA, it is fully responsible for ensuring a reliable, safe and secure NPAC. It fully expects that the contract, once negotiated, will spell out its duties in greater detail and specificity, and that Telcordia will be accountable for meeting the terms of that contract. In addition, because the Commission has the ability to designate and undesignate an LNPA, the Commission retains full authority and capability, even post-selection,

² The S²ERC study stated, “The per-carrier cost would top out at a little under \$600,000.” Eric Burger, *Issues and Analysis of a Provider Transition for the NPAC*, S²ERC TECHNICAL REPORT, at 13 (July 22, 2014) (attached as Exhibit B to Comments of Telcordia Technologies, Inc., WC Docket No. 09-109 and CC Docket No. 95-116 (Aug. 22, 2014)) (“S²ERC Report”). It also stated, “Projects of this scale run from \$250,000 to \$1,500,000” as a more general observation. S²ERC Report at 11. S²ERC in that comment was clearly addressing only the larger carriers that would need to initiate and execute enterprise IT projects. *Id.*

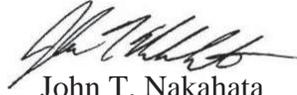
Marlene H. Dortch
October 17, 2014
Page 4 of 4

REDACTED—FOR PUBLIC INSPECTION

to ensure that the new NPAC will meet the security needs of all stakeholders, including, industry, national security agencies, public safety agencies, state public utility commissions and the Commission itself.

Please contact me if you have any questions.

Sincerely,



John T. Nakahata

*Counsel to Telcordia Technologies, Inc., d/b/a
iconectiv*

cc: Rear Admiral David Simpson (USN, ret.)
Lisa Gelb
Ken Moran
Ken Burnley
Nick Bourne
Randy Clarke
Diane Griffin Holland
Greg Intoccia
Allan Manuel
Ann Stevens
Jane Kelly
Sanford Williams