

November 14, 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 November 12, 2014, Shawn Burke, Global Chief Security Officer of Sungard Availability Services, LP (“Sungard AS”), Chris Drake, Chief Technology Officer, and Joel Zamlong, Vice President, of Telcordia Technologies, Inc., d/b/a iconectiv (“Telcordia”), Rear Admiral Jamie Barnett (USN, ret.) of Venable LLP, John Kimmins of Catapult Consultants, and I, all on behalf of Telcordia, met with Rear Admiral David Simpson (USN, ret.), Chief, Ken Moran, Deputy Chief and Greg Intoccia, Special Counsel, Cybersecurity and Communications Reliability Division, all of the Public Safety and Homeland Security Bureau.

In the meeting, we discussed that Sungard AS will be supplying and managing the hardware, software and connectivity infrastructure for Telcordia’s NPAC database, while Telcordia will be providing the application and business processes. Telcordia is the prime contractor, responsible for delivering the overall solution pursuant to the LNPA contract that it would enter into with the industry (presumably with North American Portability Management LLC (NAPM)). Sungard AS is Telcordia’s subcontractor. The relationship between Telcordia and Sungard AS will be well-defined, with service level agreements, change management and workflow/ticket tools to ensure that all work, including providing NPAC access to new entities, is authorized by Telcordia. Sungard AS will be providing Telcordia with a dedicated infrastructure that is entirely protected, with no Sungard AS access from outside of the United States. Telcordia will have its own servers with its own cages within Sungard AS’s data centers.

Sungard AS has extensive experience providing data center infrastructure services and disaster recovery for thousands of clients. Among these are clients that house and protect very sensitive data, including financial records and health care records. Sungard AS maintains a robust security system to anticipate, detect, and deter potential threats, both external and “insider,” and has a strong record of protecting the customers that it hosts. Sungard AS tests and vets its supply chain components and has lab environments in which to do so. In addition,

Ms. Marlene H. Dortch

November 14, 2014

Page 2 of 2

Telcordia will conduct its own testing in its own lab environments. These lab environments will enable both Sungard AS and Telcordia to engage in “sandboxing” when appropriate in addressing a threat. Both Telcordia and Sungard AS will be following best practices for preventing and protecting the NPAC database and associated applications. The system will have substantial redundancy both for each region and among regions, which would aid with disaster recovery.

With respect to authorizing new users, Telcordia will handle vetting the new users and establishing the appropriate access control. Once Telcordia has determined that the user is permissible, it will provide a ticket to Sungard AS to establish the appropriate access privileges.

Telcordia continued to express its willingness to work with the Bureau and federal, state, and local law enforcement and security agencies, as well as the telecommunications industry and regulators, to ensure that the NPAC database and associated applications such as the Enhanced Law Enforcement Platform are operated in a secure and reliable manner.

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.)
Ken Moran
Greg Intoccia