

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554**

In the Matter of)		
)		
NANC Recommendation of a Vendor)	Docket No.	CC 95-116
to Serve as Local Number Portability)		WC 09-109
Administrator)		

**REPLY COMMENTS OF
THE FEDERAL BUREAU OF INVESTIGATION,
THE DRUG ENFORCEMENT ADMINISTRATION,
THE UNITED STATES SECRET SERVICE, AND
U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT**

Elaine N. Lammert
Deputy General Counsel
Office of the General Counsel
Federal Bureau of Investigation
935 Pennsylvania Avenue, N.W.
Washington, D.C. 20535

Wendy H. Goggin
Chief Counsel
Office of the General Counsel
Drug Enforcement Administration
8701 Morrisette Drive
Springfield, VA 22152

Donna L. Cahill
Chief Counsel
Office of the Chief Counsel
United States Secret Service
950 H Street, N.W.
Washington, D.C. 20223

Mike Davis
Director of Enforcement and Litigation
Office of the Principal Legal Advisor
U.S. Immigration and Customs Enforcement
500 12th Street, S.W.
Washington, D.C. 20536

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554**

In the Matter of)		
)		
NANC Recommendation of a Vendor)	Docket No.	CC 95-116
to Serve as Local Number Portability)		WC 09-109
Administrator)		

**REPLY COMMENTS OF
THE FEDERAL BUREAU OF INVESTIGATION,
THE DRUG ENFORCEMENT ADMINISTRATION,
THE UNITED STATES SECRET SERVICE, AND
U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT**

The Federal Bureau of Investigation (“FBI”) and the Drug Enforcement Administration (“DEA”), law enforcement components of the U.S. Department of Justice (“DOJ”), and the United States Secret Service (“USSS”) and United States Immigration and Customs Enforcement (“ICE”), law enforcement components of the U.S. Department of Homeland Security (“DHS”) (hereafter “Federal Law Enforcement Agencies”) submit reply comments in the ongoing proceeding concerning the recommendation of the North American Numbering Council (“NANC”) that Telcordia Technologies, Inc. doing business as iconectiv (“Telcordia”) serve as the next local number portability administrator (LNPA) to assist the Commission in evaluating law enforcement, public safety, and national security issues.

While the Federal Law Enforcement Agencies take no position on either the selection of Telcordia as the LNPA vendor or the fairness of the process that resulted in the NANC recommendation of Telcordia to the Commission, it is appropriate for the Commission to consider the ability of the LNPA vendor to satisfy the important law enforcement, public safety,

and national security equities of the Federal, State, Local, and Tribal law enforcement agencies who rely on the important and highly sensitive services the LNPA provides to assist virtually all significant criminal and national security investigations.

Reliable and accurate information from the LNPA is vital to the day-to-day work of law enforcement agencies and protects the privacy interests of the public. The data the LNPA provides in response to a law enforcement query ensures that law enforcement agencies serve lawful process on the telecommunications carrier of a person reasonably believed to be engaged in criminal behavior or a national security investigation, and that law enforcement is capable of timely tracking a suspect's porting actions throughout those investigations. Otherwise, records of individuals who have committed no wrongdoing – and whose communications are of no interest to the government – could conceivably be inadvertently requested and lawfully produced by the communications provider based on erroneous information supplied by the LNPA.

I. LAW ENFORCEMENT SEEKS SAFEGUARDS CONCERNING THE LNPA VENDOR'S CAPABILITIES.

Law enforcement investigations depend on accurate information, including accurately identifying the service provider who handles a suspect's telecommunications account. Law enforcement agencies, including the FBI and DEA, typically query the system maintained by the LNPA vendor to obtain accurate current and historical information about the company who provides the service to the account so that the law enforcement agency can serve the appropriate legal process on the correct provider. Law enforcement agencies also require that their queries of the system maintained by the LNPA remain confidential so that a potential criminal will not learn that law enforcement is investigating them, which could result in an individual fleeing, destroying vital evidence of their criminal activity, or continuing to compromise national security.

The Federal Law Enforcement Agencies want to ensure that the Commission require that the LNPA vendor continues to provide, at a minimum, the same information that is currently provided by the existing LNPA vendor through a confidential query conducted over a secure web-based service in real time or near real time. The LNPA vendor must be able to provide both current and historical information for a given phone number to include: the name of the service provider; the service provider identifier or official company number (SPID or OCN); the date range of service; the service provider contact information (including a contact phone number); the alternate SPID number (in the case of a telephone number reseller); the alternate service provider, if any; and the alternate service provider contact information (including a contact phone number). This information must be available to law enforcement in real or near real time immediately upon granting the contract to the LNPA. Law enforcement cannot afford to have a lapse in this vital service, and the LNPA vendor must be able to repair and/or restore the query system used by law enforcement on a priority basis if the system fails in whole or in part. The LNPA vendor must also continue to provide an application programming interface (API) that permits a variety of platforms immediately to query large batches of such numbers from multiple locations.

The FCC needs to ensure that the LNPA vendor will not have unwarranted¹ visibility into the queries submitted by a law enforcement agency in order to maintain the confidentiality and integrity of those investigations, and the steps necessary to conduct lawful investigations. Preventing unwarranted, and potentially harmful, visibility means that the FCC cannot allow an LNPA to have remote access outside the U.S. or through a foreign corporate-parent entity, and

¹ Unwarranted” includes unauthorized access, such as access that is not authorized for diagnostic, system design, or technical support purposes, or that is facilitated through misappropriated credentials.

the LNPA vendor cannot track, log, or preserve the queries submitted by law enforcement agencies.

II. THE LNPA VENDOR MUST MAINTAIN VIGOROUS SECURITY STANDARDS.

The integrity of the system maintained by the LNPA vendor is critical to the Federal Law Enforcement Agencies. The Commission must require the LNPA vendor to maintain robust security measures and to have a written security plan that is approved by the contracting party, NAPM LLC, in consultation with Federal law enforcement and other effected agencies, and filed with the Commission,. The security plan should comply with the National Institute of Standards and Technologies (NIST) cybersecurity framework, taking into account that the Request for Proposal (RFP) to select an LNPA vendor contained technical requirements for data base security. After the final selection of the LNPA vendor, the Commission may need to work with the contracting party to address additional security requirements commensurate with the risks posed by a data base breach. The LNPA vendor must be required to file compliance and security incident reports which the FCC that are available to government entities, but anonymized if released to the public, and there should be a process for appropriate entities to conduct regularly scheduled as well as random compliance inspections. The LNPA vendor must be able to authenticate the credentials of a law enforcement agency user to access the system, and conduct audits of the system that are able to detect access to the law enforcement queries by employees or contractors of the LNPA vendor or any other third party.

Given law enforcement's concerns with the potential interference with law enforcement investigations by individuals with inside knowledge of law enforcement queries, the LNPA vendor must also provide NAPM LLC with a detailed accounting of its supply chain standards

and procedures specific to the query system maintained by the LNPA vendor, and file this report with the FCC. The FCC should retain the option to request mitigation steps related to the supply chain report. Similarly, LNPA personnel charged with the responsibility of secure network access must be U.S. citizens, capable of holding and maintaining a security clearance. The contract with the LNPA vendor must require the LNPA vendor, in coordination with law enforcement, to assess the suitability of those individuals who will have access to the number portability system.

The Federal Law Enforcement Agencies request that the Commission ensure that the LNPA vendor be required to ensure the continuity of operations of the system and establish at least one secure backup data center for such a purpose. Additionally, the LNPA vendor must not grant any administrative access or “write” privileges to individuals or entities located outside the U.S.

CONCLUSION

The Federal Law Enforcement Agencies ask the Commission to take into account these law enforcement, public safety and national security concerns when making its determination about the next LNPA vendor.

Respectfully submitted,

THE FEDERAL BUREAU OF INVESTIGATION

/s/ Elaine N. Lammert
Elaine N. Lammert
Deputy General Counsel
Office of the General Counsel
Federal Bureau of Investigation

THE DRUG ENFORCEMENT ADMINISTRATION

/s/ Wendy H. Goggin
Wendy H. Goggin
Chief Counsel
Office of the General Counsel
Drug Enforcement Administration

935 Pennsylvania Avenue, N.W.
Washington, D.C. 20535

8701 Morrisette Drive
Springfield, VA 22152

UNITED STATES SECRET SERVICE

U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT

/s/ Donna L. Cahill

Donna L. Cahill
Chief Counsel
Office of the Chief Counsel
United States Secret Service
950 H Street, N.W.
Washington, D.C. 20223

/s/ Mike Davis

Mike Davis
Director of Enforcement and Litigation
Office of the Principal Legal Advisor
U.S. Immigration and Customs Enforcement
500 12th Street, S.W.
Washington, D.C. 20536

Dated: August 11, 2014