

337

Congress of the United States
House of Representatives
Washington, DC 20515-1604

May 2, 2016

The Honorable Tom Wheeler
Chairman
Federal Communications Commission
445 12th Street, SW
Washington, DC 20554

Dear Chairman Wheeler:

As you may recall, in August of 2014, I wrote to you regarding a serious concern I had regarding the inadequate and weak security requirements contained in the Local Number Portability Administrator (LNPA) RFP. This critical infrastructure is used by our nation's 2,000 telecommunications carriers for the proper routing of nearly 10 billion calls and text messages a day, and law enforcement submits 4 million lawful requests every year to access some of this information. A recent article in the Washington Post, suggested very lax treatment of security requirements imposed on the new LNPA vendor.

It is my belief that it would have been more productive for the FCC to have written stronger security requirements into the RFP and then competed and judged the bidders with those terms in mind. Instead, we are all now waiting to see how DHS, DOJ, and the Intelligence agencies' requests will be treated under the final agreement with the new LNPA vendor.

Since the terms of the final agreement have not yet been disclosed, I can only inquire whether the security requirements match the promises made by the new vendor during the proceedings on some of the specific security terms that should be included in the contract.

I presume that if any of these commitments are not being met, you would not go forward with this process. I am further troubled that the Master Services Agreement, which presumably contains the commitments made by the parties to the contract, has now been filed under a protective order, so not only can the public not see them, but neither can I. And yet, strangely, the security documents are available, not at the FCC, but by going to the offices of the parties' attorneys. So I guess this means that you do not consider them classified but just not available to those who consider this a vital part of the LNPA responsibility.

For that reason, I am writing today to inquire what processes and procedures you have put in place to ensure that the new LNPA vendor lives up to the commitments that are outlined in the March 2015 order. Specifically, I would like your assurance that the Master Services Agreement now filed at the Commission contains the following provisions:

1. Telcordia and its subsidiaries will use a U.S- based supply chain.
2. There will be no administrator "write" privileges outside of the U.S.
3. Data will be stored only within the U.S.
4. There is a rigorous, independent audit program backed by robust enforcement tools throughout the term of the contract.
5. The U.S. NPAC will be built in America by U.S. citizens.
6. U.S. coders will be pre-screened, vetted, trained and supervised, preferably by cleared personnel.
7. All code for the U.S. NPAC will be original and will not contain code deployed in any foreign systems.
8. U.S. code will not be later deployed in any foreign system.
9. The security requests made by the FBI, DEA, US Secret Service and US Immigration and Customs Enforcement in their reply comments dated August 11, 2014 will be granted and included in the contract. Please enumerate these and describe any security requirements requested by the executive branch that were not incorporated into the LNPA contract.

With respect to recent press reports concerning the new LNPA vendor's practice of permitting foreign nationals to write computer code for the new software, I find this most troubling. I am eager to learn what steps the agency is taking to investigate these allegations to determine if they are true. Additionally, I would like to know how the national security and law enforcement requirements are being addressed during the transition to the new vendor and how they will be addressed once the transition is complete. Requirements that are not properly enforced are essentially meaningless.

Thank you in advance for your commitment to ensuring that the needed public safety and national security requirements are in place with proper enforcement mechanisms before the order implementing the Master Services Agreement is approved by the Commission.

Sincerely,



Mike Pompeo
Member of Congress

Ccs: Admiral David Simpson
FCC Commissioner Pai
FCC Commissioner Rosenworcel
FCC Commissioner Clyburn
FCC Commissioner O'Rielly



FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF
THE CHAIRMAN

July 11, 2016

The Honorable Mike Pompeo
U.S. House of Representatives
436 Cannon House Office Building
Washington, D.C. 20515

Dear Congressman Pompeo:

Thank you for sharing your views on the importance of including strong security measures in the local number portability administrator ("LNPA") Master Services Agreement ("MSA").

I understand and share your belief that security for this critical component of our communications infrastructure is paramount. From the outset of this proceeding, the Commission has taken proactive steps to ensure that the LNPA contract fully addresses and adequately mitigates any public safety, law enforcement or national security concerns. The initial Request for Proposal for the LNPA established a high level base line designed to ensure applicants be adept at meeting security and reliability requirements. Moreover, our March 27, 2015 Order provisionally selecting Telcordia d/b/a iconectiv ("Telcordia") committed to addressing the security requirements provided by Executive Branch entities with expertise in and responsibility for law enforcement and national security matters. Further, while overseeing the negotiations between the North American Portability Management LLC ("NAPM") and Telcordia on the security provisions of the MSA, the Commission required the parties to include terms and conditions in the MSA that would ensure the secure and reliable operation of the number portability system. The resulting MSA being considered by the Commission includes granular detail regarding cybersecurity, supply chain risk management, and insider threat management, among other security and reliability measures. In this respect, provisions are in place that address each of the nine considerations cited in your letter, and incorporate the National Institute Standards and Technology ("NIST") cybersecurity framework and supply chain risk management practices, as well as other standards-based requirements.

The FCC has already begun implementing a rigorous audit and inspection process in conjunction with the FBI and the North American Portability Management LLC, which will remain in place throughout the term of the contract. Further, Telcordia's Security Plan, which is included in the MSA, will evolve over time as the security threat environment evolves.

You asked for my assurance that the MSA now filed at the Commission contains the security provisions outlined in your letter. In addressing the security provisions of the

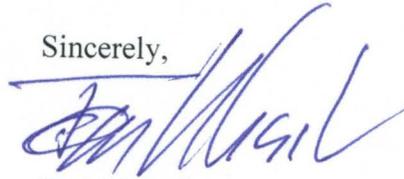
MSA, the Commission sought, and continues to seek, the most secure and reliable operation of the number portability system. While I cannot publicly comment on the specific aspects of the MSA under consideration, I can provide my assurance that the MSA addresses each of the nine provisions outlined in your letter, as noted above. In addition, I would be happy to have my staff brief you or your staff on the MSA under consideration.

You also asked how the Commission is addressing the recent reports of Telcordia's use of non-U.S. citizens to perform pre-contract work. In close coordination with the national security agencies, the Commission required and Telcordia agreed that it would discard all pre-contract work performed through the time that the Commission learned of such work. In addition, the MSA includes rigorous oversight measures and explicitly requires that only appropriately vetted U.S. citizens work on the project.

The Commission, in coordination with our federal law enforcement and national security partners and the NAPM, will continue to closely oversee the LNPA transition. Clear lines of authority, risk responsibility, and accountability are in place. Moreover, the Commission will take all appropriate steps to ensure that these security requirements continue to be met moving forward.

Again, thank you for contacting me regarding your interest in this matter. Please let me know if I can be of further assistance.

Sincerely,



Tom Wheeler