SunCom
WIRELESS

April 20, 2007

Ms. Sigal P. Mandelker
Deputy Assistant Attorney General
Criminal Division
United States Department of Justice
950 Pennsylvania Avenue, N.W.
Washington, D.C. 20530

Mr. Stewart A. Baker
Assistant Secretary for Policy
United States Department of Homeland Security
3801 Nebraska Avenue, N.W.
Washington, D.C. 20528

Ms. Elaine N. Lammert
Deputy General Counsel
Federal Bureau of Investigation
935 Pennsylvania Avenue, N.W.
Washington, D.C. 20530

Re: Pending FCC Applications ITC-T/C-20070309-00102, 0002914078, 0002914081, and ISP-PDR-20070309-00003

Dear Ms. Mandelker, Ms. Lammert and Mr. Baker:

As you know, SunCom Wireless Holdings, Inc. ("SunCom") has been discussing with the Department of Justice, the Federal Bureau of Investigation and the Department of Homeland Security (together, "the Agencies") those certain applications and the request for declaratory ruling pursuant to section 310(b)(4) of the Communications Act designated by the following FCC File numbers: ITC-T/C-20070309-00102, 0002914078, 0002914081 and ISP-PDR-20070309-00003 ("the Applications").

SunCom has indicated to the Agencies its interest in and willingness to provide certain assurances with regard to procedures applicable to law enforcement requests and the protection of its subscriber and network information, as follows:

1. SunCom has designated a point of contact who has the authority and responsibility for accepting and overseeing service of legal process and other requests for information from law enforcement agencies and maintaining the security of any information relevant to a lawful request of law enforcement. The point of contact will be available 24 hours a day, 7 days a week. SunCom shall promptly notify the Agencies of any change in its designated point of contact, shall provide to the Agencies the point of contact's contact information, and shall update this contact information as necessary. The point of contact (and any successor) shall be a resident U.S. citizen and a person SunCom reasonably believes is eligible for appropriate U.S. security clearance. In addition, SunCom shall cooperate with the Agencies in providing such information as they may reasonably

request for conducting a background check and/or security clearance process on the point of contact.

2. SunCom shall store exclusively in the U.S., if stored for any reason:

   a) Any information relating to, or the content of, communications intercepted by U.S. federal, state or local government agents within the U.S.;

   b) Any content of any communication involving a SunCom subscriber;

Provided, however, that these requirements do not apply to any such communications stored by the customer or subscriber.

   c) Subscriber transactional data (*e.g.*, call, e-mail, website or transaction data)

   d) Subscriber information (*e.g.*, name, address, billing address, type of service); and

   e) Subscriber billing records.

Provided, however, that the copies of information described in (b), (c), (d) and (e) above may be stored at a location outside of the United States for (i) the bona fide commercial request of particular customers or subscribers, or (ii) otherwise in accordance with bona fide commercial reasons of SunCom and, in either case, upon written notice to the Agencies.

3. SunCom agrees that, for all customer billing records, subscriber information, and any other related information used, processed, or maintained in the ordinary course of business relating to communications services offered in the United States ("U.S. Records"), without regard to where they are stored, Suncom will make such U.S. Records available in the United States and will produce them in response to lawful U.S. process. For these purposes, U.S. Records shall include information subject to disclosure to a U.S. Federal or state governmental entity under the procedures specified in Sections 2703(c) and (d) and Section 2709 of Title 18 of the United States Code. Suncom agrees to ensure that U.S. Records are not made subject to mandatory destruction under any foreign laws. Suncom agrees to take all practicable measures to prevent unauthorized access to, or disclosure of the content of, communications or U.S. Records, in violation of any U.S. Federal, state, or local laws or of the commitments set forth in this letter.

4. SunCom shall not, directly or indirectly, disclose or permit disclosure of, or provide access to, U.S. Records or any of the information described in paragraph 2 above, to any foreign person or government (or identified representative, component or subdivision thereof) without satisfying all applicable U.S. federal, state and local legal requirements, and obtaining the express written consent of the Agencies or the authorization of a court of competent jurisdiction in the United States. Any request for any such information, or any request for confidential, non-public information concerning SunCom's network

operations, submitted by any foreign person or government (or identified representative, component or subdivision thereof) shall be referred to the Agencies as soon as possible and in no event later than five (5) business days after such request.

These assurances will be effective immediately upon consummation of the transaction described in the Applications.

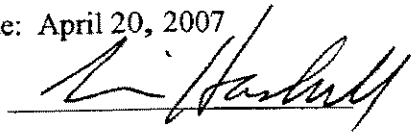
The assurances provided in this letter reflect SunCom's commitment to maintaining secure facilities in the United States, as well as SunCom's desire to continue its strong working relationship with the U.S. government. Should there be any material changes with respect to SunCom's security arrangements; SunCom will promptly notify the Agencies.

Should you have any questions regarding any aspect of this letter, please do not hesitate to contact the undersigned.

Very truly yours,

SunCom Wireless Holdings, Inc.

Date: April 20, 2007

By: 

Printed Name: Eric Haskell

Title: Executive Vice President and CFO