NNMT
Northern New Mexico Telecom

February 21, 2013

Ms. Marlene H. Dortch
Office of the Secretary
Federal Communications Commission
445 12th Street, S.W.
Washington, DC 20554

Re: Northern New Mexico Telecom
Certification of CPNI Filing
EB Docket 06-36
Electronically filed via ECFS

Dear Ms. Dortch:

In compliance with the FCC's EB Docket 06-36, Northern New Mexico Telecom hereby files its report providing its annual CPNI officer certification and accompanying statement explaining how its operating procedures ensure compliance with the FCC's CPNI rules.

Should you have any questions or need additional information, please contact the undersigned.

Sincerely,

DANNY GRAY
General Manager

amp

P.O. Box 269 Mora, NM 87732-0269 575.387.2216 FAX: 575.387.9010

NNMT
Northern New Mexico Telecom

ANNUAL CERTIFICATE OF COMPLIANCE
WITH CPNI REGULATIONS

I, Danny Gray, an officer of Northern New Mexico Telecom (hereinafter "the Company"), do hereby certify based upon my personal knowledge that the Company has established operating procedures that are adequate to ensure compliance with the rules in 47 C.F.R. §§ 64.2001-64.2011. The statement accompanying this certificate explains how the Company's operating procedures ensure that it is in compliance with those rules.

Officer's signature: _____

Date: 02/21/2013

P.O. Box 269 Mora, NM 87732-0269 575.387.2216 FAX: 575.387.9010

Annual 47 C.F.R. Section 64.2009(e) CPNI Certification
EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2013 covering the prior calendar year 2012

Date Filed: February 21, 2013

Name of company covered by this certification: Northern New Mexico Telecom

Form 499 Filer ID: 821642

Name of signatory: Danny Gray

General Manager

I, Danny Gray, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. *See* 47 C.F.R. Section 64.2001 *et seq.*

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements set forth in section 64.2001 *et seq.* of the Commission's rules.

The company has not taken any actions (proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year. Companies must report on any information that they have with respect to the processes pretexters are using to attempt to access CPNI, and what steps companies are taking to protect CPNI.

The company has not received any customer complaints in the past year concerning the unauthorized release of CPNI (number of customer complaints a company has received related to unauthorized access to CPNI, or unauthorized disclosure of CPNI, broken down by category or complaint, *e.g.* instances of improper access by employees, instances of improper disclosure to individuals not authorized to receive the information, or instances of improper access to online information by individuals not authorized to view the information).

Signed _____

Attachments: Accompanying Statement explaining CPNI procedures

Customer Proprietary Network Information (CPNI)

Purpose

1. These operating procedures are designed to ensure compliance with the FCC's CPNI rules (47 CFR 64.2001-64.2011) per Section 222 of the Communications Act of 1934, as amended
2. This operating procedure will govern the process of handling customer requests related to CPNI.
3. Annually review CPNI policy statement with all employees
4. Annually file CPNI compliance filings with the FCC
5. Definitions related to FCC CPNI rules are contained in Part 64.2003

Customer Notification

1. The Company will notify and inform each Customer of his or her right to restrict the use or disclosure of, and access to, CPNI
2. The Company will maintain records of that notification, whether oral or written, for at least one year
3. The notification will provide information sufficient to enable our Customers to make informed decisions as to whether to permit the use or disclosure of, or access to, their CPNI
4. The notice will contain a statement that the Customer has a right, and we have a duty, under federal law, to protect the confidentiality of their CPNI
5. The notice will specify the types of information that constitute CPNI and the specific entities that will receive CPNI, describe the purposes for which the CPNI will be used, and inform the Customer of his or her right to approve or disapprove those uses and deny or withdraw access to CPNI use at any time. With regard to the latter, we indicate that any approval, or disapproval, will remain in effect until the Customer affirmatively revokes or limits such approval or denial
6. The Company will advise the Customer of the precise steps the Customer must take in order to grant or deny access to CPNI and clearly state that a denial of approval will not affect the provision of any services to which the Customer subscribes
7. The statement will be in a clear and neutral language, which describes the consequences directly resulting from the lack of access to CPNI. In addition, we may state that the Customer's consent to use his or her CPNI may enhance our ability to offer products and services tailored to meet the Customer's needs and that we will disclose the Customer's CPNI to any person upon the affirmative written request of the Customer
8. For non-English speaking customers, should portions of a notice be translated into another language, then all portions of the notice are translated into that language
9. The notification will not include any statement that attempts to encourage a Customer to freeze third-party access to CPNI
10. New Customers will be verbally notified at the time of the request for service
11. In addition, a CPNI statement will be included in our new customer Welcome Packets

Use of CPNI

1. The Company will use, disclose or permit access to CPNI to protect our rights, property, Customers, and other carriers from fraudulent, abusive or unlawful use of, or subscription to, our services

2. The Company will use, disclose or permit access to CPNI to provide or market service offerings among the different categories of service – local, interexchange, etc. to which the Customer already subscribes
3. When the Company provides different categories of service, and a Customer subscribes to more than one service category, we may share the Customer's CPNI with the affiliate that provides service to the Customer; but if a Customer subscribes to only one service category, we do not share the Customer's CPNI with an affiliate without the Customer's approval
4. We use, disclose or permit access to CPNI derived from our provision of local exchange or interexchange service for the provision of CPE and call answering, voice mail or messaging, voice storage and retrieval services, and protocol conversion, without Customer approval
5. Without Customer approval, we do not use, disclose or permit access to CPNI to provide or market service offerings within a category of service to which the Customer does not already subscribe, except that we use, disclose or permit access to CPNI to do the following:

   A. Provide inside wiring installation, maintenance and repair services
   B. Services such as, but not limited to, speed dialing, computer-provided directory assistance, all monitoring, call tracing, call blocking, call return, repeat dialing, call tracking, call waiting, caller ID, call forwarding, and certain Centrex features

6. The Company will not use, disclose or permit access to CPNI to identify or track Customers that call competing service providers. For example, as a local exchange carrier we do not use local service CPNI to track Customers that call local service competitors
7. Should our company provide CMRS or VoIP services, we will comply with Part 64.2005(b) as these rules relate to these services

Approval or Disapproval of CPNI

1. We honor a Customer's approval or disapproval until the Customer revokes or limits such approval or disapproval
2. Other Opt-In provisions per Part 64.2008(e) will be followed
3. If we disclose or allow access to Customers' individually identifiable CPNI to our affiliates, we will require, in order to safeguard that information, confidentiality agreements that:

   A. Require our affiliates' use of the CPNI only for the purpose of marketing or providing the communications-related services for which the CPNI has been provided
   B. Disallow their permitting any other party to use, allow access to, or disclose the CPNI to any other party, unless they are required to make disclosure under force of law
   C. Require that they have in place appropriate protections to ensure the ongoing confidentiality of the CPNI

Customer Authentication for Call Detail

1. Since the release of call detail information over the telephone presents an immediate risk to privacy, the Company is prohibited from releasing call detail information based

on customer-initiated telephone contact, except under four circumstances:

A. When a customer provides a pre-established password
B. When a customer requests that the information is sent to the customer's address of record
C. When a representative of our company calls the telephone number of record and discloses the information
D. At retail locations, we may continue to provide account access to customers who present valid photo IDs

2. Password protection is not required for routine customer care procedures regarding service/billing disputes or questions if the customer is able to provide all of the call detail information necessary to address the customer question (i.e., telephone number called, when it was called, amount charged for the call)

3. In addition, the Company will provide mandatory password protection in the event that online account access is allowed. Online access based solely on a customer's readily available biographical information is prohibited. However, the Company is not required to reinitialize existing passwords for online customer accounts

Establishing a Password

1. For existing customers, the Company must first authenticate the customer by either calling the account number on record or the customer presenting a valid photo id, in person at any retail location
2. Existing customers may establish or update password information using a form sent by the Company to the customer address of record
3. For a new customer, the Company may establish a password at the time of service initiation and the customer may be authenticated at that time

Customer Account Authentication

1. We will authenticate the customer for their protection and confirm the person we are speaking with is the account holder. Authentication may include, but is not limited to the following:

A. Last four digits of the Social Security Number
B. Mother's maiden name
C. City of birth
D. Year of birth
E. Childhood pet
F. Other names listed on the account

2. We will not discuss the following account information with a spouse, child, parent, etc.; unless they are authorized by the account holder. Account information may include, but is not limited to, the following:

A. Name
B. Address
C. Phone number
D. Billings or charges
E. Balance due or payment status

3. A maximum of four authorized contacts may be added to the account by the authorized account holder

4. All documents, notes, and printed materials with customer information will be shredded and disposed of properly. This may include, but is not limited to the following:

   A. Social Security Number
   B. Customer's name, address, phone number
   C. Copy of bill or remittance slip

Law Enforcement

1. All requests for customer account or billing information will be directed to the Human Resources Manager or another member of the Human Resources Department

Notice of Account Changes

1. The Company must notify a customer immediately of account activity, such as a change to a password, online account, or address of record. Notification may be sent by email, voicemail, text message, or US Mail to the customer's address of record

Notice of Unauthorized Disclosure or Breach of CPNI

1. If there has been a breach of CPNI, the Company must provide electronic notification of the breach within seven business days to the United States Secret Service ("USSS") and the Federal Bureau of Investigation ("FBI"). (The FCC will provide a link for the reporting of breaches at www.fcc.gov/eb/CPNI/.) In order to allow law enforcement time to conduct an investigation, the Company must wait another seven business days before notifying the affected customers of the breach (unless the USSS and FBI request that the carrier continue to postpone disclosure). However, the Company may notify customers sooner if there is a risk of immediate and irreparable harm. In addition, we must keep records of discovered breaches for at least two years

Joint Venture and Independent Contractor Use of CPNI

1. The Company must obtain opt-in consent from a customer before disclosing a customer's CPNI to a joint venture partner or an independent contractor for the marketing of communications-related services to the customer

Business Customers

1. The Company may establish contract authentication procedures for business customers that are different from residential customers, so long as those customers have a dedicated account representative and the contracts specifically address the protection of CPNI

CPNI Compliance

1. The Company has implemented a system by which the status of a Customer's CPNI approval can be clearly established prior to the use of the CPNI
2. We have trained our personnel as to when they are and are not authorized to use CPNI

3. Any unauthorized use, sale, or otherwise disclosure of CPNI by any employee would subject the employee to disciplinary action. For the first violation, an employee will be given a warning and the violation will be noted on the employee's record. An employee will be subject to termination of employment for a second violation
4. The Company employees will sign a CPNI Policy Acknowledgement that will be placed in the employee's personnel file
5. The Company maintains a record of our own and our affiliates' sales and marketing campaigns that use Customers' CPNI. The record includes a description of each campaign, the specific CPNI that was used in the campaign, and what products and services were offered as part of the campaign. We retain these records for at least one year
6. Notification records and approval or disapproval records need to be retained for at least one year
7. The Company has established a supervisory review process regarding compliance with the CPNI rules for outbound marketing situations and we maintain compliance records for at least one year. Specifically, our sales personnel obtain supervisory approval of any proposed outbound marketing request for Customer approval of the use of CPNI
8. The Company has a corporate officer who acts as agent for the Company and signs a compliance certificate on an annual basis before March 1 of each year in EB Docket No. 06-36 stating that the officer has personal knowledge that the Company has established operating procedures adequate to ensure compliance with applicable CPNI rules. We provide a statement accompanying the certificate that explains our operating procedures and demonstrates compliance with the CPNI rules. In addition, we will include an explanation of any actions taken against data brokers and a summary of all customer complaints received in the past year concerning the unauthorized release of CPNI

COMPANY: Northern New Mexico Telecom

Officer

02/21/2013

Date