502 Main Street
P O Box 130
Union, IA 50258-0130

HEART of IOWA
Communications Cooperative

phone 641-486-2211
fax 641-486-2205
www.heartofiowa.coop

January 21, 2010

Marlene H. Dortch, Secretary
Office of the Secretary
Federal Communications Commission
445 12th Street, S.W., Suite TW-A325
Washington, D.C. 20554

RE: Certification of CPNI Filing, March 1, 2010
FCC Docket EB 06-36
EB-06-TC-060
Heart of Iowa Communications Cooperative

Dear Secretary Dortch:

In accordance with the Public Notice issued by the Enforcement Bureau on February 2, 2006 (DA 06-258), attached please find Heart of Iowa Communications Cooperative's annual compliance certificate for the most recent period, as required by section 64.2009(e) of the Commission's Rules, together with a statement of its operating procedures established to ensure compliance with the Commission's Rules and Regulations regarding Customer Proprietary Network Information (Attachment A).

Should you have any questions regarding this filing, please direct them to the undersigned at 641-486-2211 or e-mail executive@heartofiowa.coop.

Sincerely,

Bryan Amundson, General Manager
Heart of Iowa Communications Cooperative

Cc: Federal Communications Commission, Enforcement Bureau, Telecommunications Consumers Division, 445 12th Street, SW, Washington, DC 20554 (2 copies)
Best Copy and Printing, Inc., 445 12th Street, Suite CY-B402, Washington, DC 20554 (1 copy)

502 Main Street
P O Box 130
Union, IA 50258-0130

HEART of IOWA
Communications Cooperative

phone 641-486-2211
fax 641-486-2205
www.heartofiowa.coop

**Annual 47 C.F.R. § 64.2009(e) CPNI Certification**

**EB Docket 06-36**

Annual 64.2009(e) CPNI Certification for 2009

Date filed: January 21, 2010

Name of company covered by this certification: Heart of Iowa Communications Cooperative

Form 499 Filer ID: 804675

Name of signatory: Bryan Amundson

Title of signatory: General Manager

I, Bryan Amundson, 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. § 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 _____

Attachment A
Statement Concerning Procedures Ensuring Compliance with CPNI Rules
(Statement of Procedures Attached)

The operating procedures of Heart of Iowa Communications Cooperative (Form 499 Filer ID No. 804675) (the "Company") ensure that the Company complies with Part 64, Section 2001 *et.seq.* of the FCC rules governing the use of Customer Proprietary Network Information ("CPNI").

The Company has established a system by which the status of a customer's approval for the use of CPNI can be clearly established prior to use of CPNI. The Company relies on the involvement of its supervisor/management to ensure that no use of CPNI is made without review of applicable rules and law.

The Company trains it personnel regarding when they are authorized to use CPNI, as well as when they are not authorized to use CPNI. Personnel must sign a verification form stating that they have completed training and understand that any infraction of the CPNI procedures can result in disciplinary action being taken against them.

The Company has an express disciplinary process in place for personnel who create or are involved in an infraction of the CPNI rules and the Company's CPNI Operating Procedures.

The Company maintains records of its own sales and marketing campaigns via a log. These records include a description of each campaign, the specific CPNI used in the campaign, and the products and services that were offered as a part of the campaign. The Company has a supervisory review process for all outbound marketing. The marketing campaign log requires a supervisor to review, sign and date the log. These records are maintained for a minimum of one year.

The Company maintains records of customer approval for the use of CPNI that include a copy of the notice and the customer's "opt-out" written notification. These records are maintained for a minimum of one year.

The Company requires that customers be authenticated at the beginning of all customer initiated calls, online transactions, or in-store visits. In store visits require a valid photo ID.

The Company maintains a log of unauthorized use of CPNI, where law enforcement is required to be notified. This includes the date of discovery, notification to law enforcement, description of the breach, circumstances of the breach and a supervisor's signature and date. This log is maintained for a minimum of two years.

# STATEMENT OF PROCEDURES ADOPTED BY HEART OF IOWA COMMUNICATIONS COOPERATIVE TO ENSURE COMPLIANCE WITH THE RULES AND REGULATIONS OF THE FEDERAL COMMUNICATIONS COMMISSION REGARDING THE PROTECTION OF CUSTOMER PROPRIETARY NETWORK INFORMATION ("CPNI")

Prefatory Statement: Our Company has elected not to utilize or provide CPNI for any purpose other than those purposes that are permissible without customer approval in accordance with Section 64.2005 of the FCC's Rules and Regulations. We provide our customers notification of their rights with respect to their CPNI and we have adopted the procedures set forth below to ensure our familiarity and compliance with the applicable rules in the event that we subsequently elect to utilize or provide CPNI for any purpose that requires customer approval.

**CPNI Use**

(1) We recognize that we may use, disclose or permit access to CPNI to protect our rights and property, our Customers, and other carriers from fraudulent, abusive or unlawful use of, or subscription to, our services.
(2) We understand that we may use, disclose or permit access to CPNI to provide or market service offerings among the categories of service to which the Customer already subscribes. When we provide different categories of service, and a Customer subscribes to more than one service category, we understand that 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 may not share the customer's CPNI with an affiliate without the Customer's approval.
(3) We understand that we may 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, fax store-and-forward, and protocol conversion, without Customer approval.
(4) In the absence of 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 understand that we may use, disclose or permit access to CPNI to: (a) provide inside wiring installation, maintenance and repair services; and (b) market, when we provide local service, services formerly known as adjunct-to-basic services such as, but not limited to, speed dialing, computer-provided directory assistance, call monitoring, call tracing, call blocking, call return, repeat dialing, call tracking, call waiting, caller ID, call forwarding, and certain Centrex features.

(5) We do 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.

**Required Procedures to Obtain Customer Approval to Use CPNI**

(1) In the event that we seek to utilize, disclose or permit access to CPNI in an instance where Customer approval is required, we will obtain approval through written, oral or electronic methods. If we rely on oral approval, we understand we bear the burden of demonstrating that such approval was given in compliance with the CPNI rules. We will honor a Customer's approval or disapproval until the Customer revokes or limits such approval or disapproval. We will maintain all records of Customer approvals for at least one year.

Subject to "opt-out" approval requirements, we understand that we may use a Customer's individually identifiable CPNI to market communications related services to that Customer, and that we may disclose that CPNI to our affiliates that provide communications-related services.

**CPNI Notice Requirement Procedures**

(1) We individually notify and inform each Customer of his or her right to restrict the use or disclosure of, and access to, CPNI. In the event that we seek to utilize, disclose or permit access to CPNI in an instance where Customer approval is required, we will solicit approval, and we will maintain records of notification, whether oral, written or electronic, for at least one year.
(2) In the event that we seek to utilize, disclose or permit access to CPNI in an instance where Customer approval is required, our notifications 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. Our notifications will: (a) contain a statement that the Customer has a right, and we have a duty, under federal law, to protect the confidentiality of CPNI; (b) 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 disapprove those uses and deny or withdraw access to CPNI use at any time. With regard to the latter, we will indicate that any approval, or disapproval, will remain in effect until the Customer affirmatively revokes or limits such approval or denial.
(3) In the event that we seek to utilize, disclose or permit access to CPNI in an instance where Customer approval is required, we will advise the Customer of the precise steps the Customer must take in order to grant or deny access to CPNI, and we will clearly state that a denial of approval

will not affect the provision of any services to which the Customer subscribes. We understand that in any such notification we may also provide a brief statement, in clear and neutral language, that describes the consequences directly resulting from the lack of access to CPNI. In addition, we understand that 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.

(4) In the event that we seek to utilize, disclose or permit access to CPNI in an instance where Customer approval is required, our notifications will be comprehensible and not misleading and, if written, will be legible, sufficiently in large type, and placed in an area readily apparent to the Customer. And, if any portion of any such notification is in another language, all portions of the notification will be in that language.

(5) We will not include in any such notification any statement that attempts to encourage a Customer to freeze third-party access to CPNI.

(6) For "opt-out" approvals, we understand that our notifications will satisfy items (1) – (5) above. We will not use oral notifications except in the event that a need arises to obtain limited, one-time use of CPNI for inbound and outbound customer telephone contacts for the duration of the call, regardless of whether we use "opt-out" or "opt-in" approval based on the nature of the contact. When we use oral notice in this manner, we will comply with items (1) – (5) above, except that, if none of the following situations are relevant to the limited use for which we seek CPNI, we will not: (a) advise Customers, if they have opted out previously, that no action is needed to maintain the "opt-out" election; (b) advise Customers that we may share CPNI with our named or unnamed affiliates or third parties if the limited CPNI usage does not result in use by, or disclosure to, an affiliate or third party; (c) disclose the means by which a Customer can deny or withdraw future access to CPNI, so long as we explain that the scope of the approval is limited to one-time use; and (d) disclose the precise steps a Customer must take to grant or deny access to CPNI, so long as we clearly communicate that the Customer can deny access to his or her CPNI for the call.

(7) In addition, for "opt-out" approvals, we understand that we must wait at least 30 days after giving Customers notice and an opportunity to opt-out before assuming Customer approval to use, disclose, or permit access to CPNI and notify Customers of the applicable waiting period for a response before approval is assumed. In the event that we utilize the opt-out mechanism, we will provide notices to customers every two years.

(8) For electronic notifications, we recognize that the waiting period begins to run on the date the notification is sent and for mail notifications, it begins to run on the third day following the date the notification was mailed. In the event we utilize e-mail to provide opt-out notices, in addition to other requirements, we will: (a) obtain express, verifiable, prior approval to

sending notices by e-mail regarding a Customer's service in general or their CPNI in particular; (b) allow Customers to reply directly to e-mails in order to opt-out; (c) use another means of communicating the notice if the e-mail is returned as undeliverable before considering the Customer to have received notice; and (d) ensure that the subject line in the e-mail clearly and accurately identifies the subject matter of the e-mail.

(9) In the event that we use "opt-out" approvals, we will also make available to every customer a method to opt-out that is of no additional cost to the Customer and is available 24 hours a day, seven days a week. We may satisfy this requirement through a combination of methods, but we allow Customers to opt-out at no cost and whenever they choose.

**CPNI Safeguard Procedures**

(1) As described in this section, we have 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) On customer initiated calls requesting call detail records (CDRs) and/or account information, a password is required in order to release the information over the phone. If the customer wishes to establish a password, the customer is first authenticated. For new customers, this will be done when the customer applies for service. For existing customers, we will either call the customer back on the telephone number listed on the account or have the customer stop in and present a valid photo id. Once the customer has been authenticated, we will ask the customer to provide a password and answer a back-up question. The password must be at least six characters in length consisting of a mixture of letters and numbers and is at the customer's discretion. Once the password has been established, they will be given the option to answer a back-up question. This question is only asked if the customer forgets his/her password. In the event that the customer answers both the password and back-up question incorrectly, the customer must be re-authenticated and create a new password/back-up question.

(3) If a customer does not wish to establish a password, the customer is informed that we can call them back at the telephone number of record, send the information to the address on account and/or have them stop into one of our business office locations and present a valid photo identification.

(4) In the event that an account holder wishes to grant permission for another person(s) to access his/her account, an Authorization form must be completed by the account holder before any information will be disclosed. It is the account holder's responsibility to give the person(s) with permission a password if calling in the office.

(5) We have trained our personnel as to when they are, and are not, authorized to use CPNI, and we have an express disciplinary process in place.

(6) We will maintain a record of any instance of our own and our affiliates' sales and marketing campaigns that use Customers' CPNI. In the event that we utilize, disclose, or permit access to CPNI in accordance with a Customer's approval, we will maintain a record of all such instances where CPNI was disclosed or provided to third parties or where third parties were allowed access to CPNI. The record will include 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 will retain these records for at least one year.

(7) We have established a supervisory review process regarding compliance with the CPNI rules for outbound marketing situations and, in the event that we seek to utilize, disclose or permit access to CPNI for outbound marketing situations, we will maintain compliance records for at least one year. Specifically, our sales personnel are required to obtain supervisory approval of any proposed outbound marketing request for customer approval of the use of CPNI.

(8) A corporate officer who acts as agent for the Company will sign a compliance certificate on an annual basis stating that the officer has personal knowledge that the Company has established these operating procedures adequate to ensure compliance with applicable CPNI rules. In addition to this certificate, 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 will be included in the annual filing. This Statement of Procedures, which sets forth our operating procedures and demonstrates compliance with the CPNI rules, will be maintained together with the compliance certificate, the explanation of any actions taken against data brokers and the summary of customer complaints.

(9) In the event that we seek to utilize, disclose or permit access to CPNI in an instance where Customer approval is required, and we utilize an opt-out mechanism, we will provide written notice within five business days to the FCC of any instance where the opt-out mechanisms do not work properly to such a degree that consumers' inability to opt-out is more than an anomaly. Any such notice will be provided in the form of a letter that will include our Company's name, a description of the opt-out mechanism(s) used, the problem(s) experienced, the remedy proposed and when it will be/was implemented, whether relevant state commission(s) were notified and what action was taken, a copy of any notice provided to customers, and contact information. We will submit any such notice even if other methods by which consumers may opt-out are offered.

(10) In the event of a breach of CPNI, United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI) will be notified electronically

via the central reporting facility at http://www.fcc.gov/eb/cpni within seven (7) business days. Notification will be given to the customer depending on the circumstance. If the breach is deemed necessary and the Company and investigating agency agree, the customer will be notified immediately. If the investigating agency finds it necessary to delay the notification in order not to impede the investigation, the customer will be notified up to 30 days following the breach (may be longer if deemed necessary). For all other breaches, the customer will be notified once seven full business days have passed.

## REVIEW AND REVISION OF PROCEDURES

**We shall undertake the responsibility of reviewing these procedures on a continuing basis to ensure compliance with all Rules and Regulations regarding the utilization of CPNI. We shall revise these procedures on a timely basis to reflect any subsequent revisions to the applicable Rules and Regulations addressing CPNI.**

Created: February 2, 2006
Revised: January 21, 2010