WOMBLE
CARLYLE
SANDRIDGE
& RICE
A PROFESSIONAL LIMITED
LIABILITY COMPANY

1401 Eye Street, NW
Seventh Floor
Washington, DC 20005

Telephone: (202) 467-6900
Fax: (202) 467-6910
www.wcsr.com

Jennifer M. Kashatus
Attorney
Direct Dial: (202) 857-4506
Direct Fax: (202) 261-0006
E-mail: JKashatus@wcsr.com

March 3, 2008

VIA ECFS

Marlene Dortch
Secretary
Federal Communications Commission
445 12th Street, SW
Washington, D.C. 20005

Re: M5 Networks, Inc., FCC Filer ID 826018, EB Docket No. 06-36

Dear Ms. Dortch:

M5 Networks, Inc. through its undersigned counsel and in accordance with the Commission's *Public Notice* DA 08-171 in the above-referenced docket, respectfully submits its annual Customer Proprietary Network Information Certification and accompanying statement.

Please contact me if you have any questions regarding this filing.

Respectfully submitted,

WOMBLE CARLYLE SANDRIDGE & RICE
A Professional Limited Liability Company

Jennifer M. Kashatus

Jennifer M. Kashatus

cc: Best Copy & Printing (via email)

Annual 47 C.F.R. § 64.2009 CPNI Certification

EB Docket No. 06-36

Annual 64.2009(e) CPNI Certification for 2007

Date filed: February 29, 2008

Name of Company covered by this certification: M5 Networks, Inc.

Form 499 Filer ID: 826018

Name of Signatory: Dan Hoffman

Title of Signatory: President & CEO

I, Dan Hoffman certify that I am an officer of M5 Networks, Inc. ("M5"), and acting as an agent of M5, that I have personal knowledge that the company has established operating procedures and policies in place that are designed to ensure compliance with the Federal Communication Commission's ("Commission") 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 are designed to maintain compliance with the Commission's CPNI rules.

M5 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 in the past year. M5 does not have knowledge of any data breaches that occurred in 2007.

M5 has taken measures to discover and to protect against attempts to gain unauthorized access to CPNI. M5 has not discovered any information about the processes that pretexters are using to attempt to gain access to CPNI, other than the publicly available procedures identified in this docket. As mentioned in Attachment A, M5 has taken several measures to safeguard CPNI, including, without limitation, conducting training regarding the appropriate use of CPNI, maintaining customer verification processes, and implementing network security measures.

M5 did not receive any complaints in the past year concerning the unauthorized release of CPNI.

Signed _____
Dan Hoffman

February 29, 2008

ATTACHMENT A

M5 NETWORKS, INC.

STATEMENT OF CPNI OPERATING PROCEDURES

M5 Networks, Inc. ("M5") is an interconnected voice-over-internet-protocol ("VoIP") provider offering and providing services to business customers throughout the United States. M5 has established policies and procedures designed to ensure that it is in compliance with the Federal Communications Commission's ("Commission") rules set forth in section 64.2001 *et seq.*, 47 C.F.R. § 64.2001 *et seq.* pertaining to the use, disclosure, and access to customer network proprietary information ("CPNI"). M5 provides this statement pursuant to section 64.0009(e) of the Commission's rules, 47 C.F.R. § 64.0009(e), to summarize the operational procedures and policies.

Permissible Use/Disclosure/Access to CPNI:

Subject to limitations set forth in its internal policies, M5 may use, disclose, and/or permit access to CPNI without obtaining customer consent for the following purposes:

- To initiate, render, bill and collect for the services it provides;
- To protect our rights and property, or to protect our customers or other carriers from fraudulent, abusive, or unlawful use or, or subscription to, such services;
- To provide inbound telemarketing, referral, or administrative services to the customer for the duration of the call, if the customer initiated the call and the customer approves the use of such information;
- To market services to customers within the same category of services to which the customer already subscribes;
- For the provision of services necessary to, or used in, the provision of such telecommunications services, including the publishing of directories; and
- As required by law, such as by a validly issued subpoena.

M5 uses CPNI in each of these categories only as is necessary.

Employee Training/Disciplinary Process:

As explained above, M5 does not use, disclose or permit access to its customer's CPNI except as permitted without customer approval or as otherwise provided by law.

M5 trains its personnel as to what information is classified as CPNI and when they are authorized and not authorized to use this information. M5 also trains its personnel regarding acceptable verification procedures and each of the topics addressed in this statement.

M5 has established a CPNI Compliance Officer and a point of contact for any CPNI-related questions.

M5 has an express disciplinary process in place for the misuse of CPNI, which includes the potential for termination.

Data Security Breaches:

M5 has procedures in place to notify the United States Secret Service and the Federal Bureau of Investigation in the event of a data breach. M5 will notify these entities through the portal listed on the FCC's website at www.fcc.gov/eb/cpni. Unless law enforcement directs otherwise, M5 will notify affected customers of the breach as soon as practicable after the expiration of the seven business day waiting period. M5 will maintain a record in accordance with section 64.2011(d) of any breaches discovered, notifications made to law enforcement, and notifications made to customers for at least two years.

Use of CPNI for Marketing Purposes:

M5 may use CPNI to market products and services to customers within the same category of service to which the customer already subscribes. M5 has established a supervisory review process for all sales and marketing campaigns for which the sales personnel seek to use CPNI. In accordance with this process, all sales and marketing campaigns must receive prior approval from a designated point of contact. When seeking approval, employees must provide a proposed description of the marketing campaign, the CPNI that will be used as part of the marketing campaign, and the products and services that will be offered as part of the campaign. M5 will maintain a record of all marketing campaigns that use CPNI for the period specified in the FCC's rules.

M5 currently does not use, disclose, and/or permit access to CPNI to market products and services to customers outside of the category of services to which the customer currently subscribes. If M5 at a later time seeks to do so, it will provide the requisite notice and obtain consent as required in sections 64.2007, 64.2008, and 64.2009 of the FCC's rules.

Authentication and Protection From Pretexting:

M5 has implemented authentication and verification procedures for incoming calls, customer service representative initiated calls, and online customer access. M5 has implemented password protection for online access that does not rely on the use of readily available biographical information or account information. M5 also has instituted procedures for addressing lost or stolen passwords.

M5 directs its employees to take measures to discover any activity that is indicative of pretexting.

It is M5's policy to prohibit the release of any CPNI, including call detail information, during an in-bound call. If the caller requests call detail information, an M5 representative either will call

the customer back at the telephone number of record or send the requested call detail information to an established address of record.

Notification of Account Changes:

M5 will notify customers immediately of the following changes to customer accounts: (1) change in the customer's password; (2) change in the customer's address of record; (3) change of the customer's online account; and (4) change in the back-up authentication information.

Tracking Customer Complaints:

M5 tracks all customers complaints that it receives regarding the improper use, disclosure, or access to CPNI. If a representative receives a customer complaint alleging the misuse of CPNI, they must log that complaint, and refer that complaint to the legal department.

Additional Security Protections:

M5 has network security measures to safeguard CPNI, including, but not limited to, encryption. M5 also has implemented role-based security measures, pursuant to which personnel have access only to information that is necessary for their particular position.