

# CM CINNAMON MUELLER

A Professional Limited Liability Company

307 North Michigan Avenue, Suite 1020  
Chicago, Illinois 60601  
Telephone: 312-372-3930  
Facsimile: 312-372-3939

Scott C. Friedman  
Admitted in Illinois and Wisconsin

Received & Inspected

FEB 17 2011

Washington, D.C. Office  
1333 New Hampshire Ave, NW, Fl 2  
Washington, DC 20036

February 14, 2011

Marlene Dortch  
Secretary  
Office of the Secretary  
Federal Communications Commission  
9300 East Hampton Drive  
Capitol Heights, MD 20743

**via Federal Express**  
Confirmation #: 796761200425

**Re: ET Docket No. 04-295; Conway Corporation ("Conway");  
Systems Security and Integrity ("SSI") Plan update**

Dear Ms. Dortch:

On behalf of Conway, we enclose an original and four copies of the company's updated SSI Plan to be filed in ET Docket No. 04-295. Conway Corporation filed an SSI plan in ET Docket No. 04-295 on March 8, 2007. The updated plan reflects changes to Conway's CALEA Compliance Officers.

We have also included an additional copy of the updated SSI Plan and ask that you date-stamp it and return it in the enclosed postage-paid envelope.

Please contact me at (312) 372-3930 with any questions. Thank you.

Regards,



Scott C. Friedman

Enclosures

cc: Bill Bethea (via email: [bill.bethea@conwaycorp.com](mailto:bill.bethea@conwaycorp.com))  
David Ward (via USPS First-Class Mail)

No. of Copies rec'd  
List A B C D E

0+4

FEB 17 2011

HCC Mail Room

## CONWAY CORPORATION'S SYSTEMS SECURITY AND INTEGRITY PLAN

The Communications Assistance for Law Enforcement Act ("CALEA") contains provisions limiting law enforcement's interception of communications and access to call-identifying information. Specifically, CALEA requires telecommunications carriers to ensure that any interception of communications or access to call-identifying information that takes place on the carrier's premises be activated only in accordance with a court order or other lawful authorization, and that a selected carrier employee authorize the interception or access. CALEA is applicable to facilities-based broadband Internet access services beginning May 14, 2007.

This Plan sets out Conway Corporation's procedures and policies for complying with these CALEA requirements for its facilities-based broadband Internet access services.

### 1. Definitions.

**Appropriate legal authorization.** A court order signed by a judge or magistrate, or other authorization (such as a subpoena or warrant) pursuant to federal or state statute, authorizing the interception of a Conway Corporation customer's communications or access to call-identifying information ("CII"). Examples of appropriate legal authorization are set forth on Exhibit 1.

**Appropriate carrier authorization.** Authorization by the CALEA Compliance Officer allowing personnel to enable law enforcement officials to intercept communications or access CII.

**Call-identifying information.** In the broadband context, call-identifying information is as defined by industry standard-setting bodies and law enforcement agencies.

**Government.** The government or any agency of the United States, or any State or political subdivision authorized to conduct electronic surveillance - usually a federal or state law enforcement agency ("LEA").

### 2. Interception of communications and access to call-identifying information.

Conway Corporation personnel **shall not** permit government entities to intercept customer communications or to access call-identifying information without appropriate authorization. Appropriate authorization includes: (i) appropriate legal authorization; and (ii) the authorization of Conway Corporation's CALEA Compliance Officer.

Any such requests by a government entity must be immediately referred to Jason Hansen, Conway Corporation's CALEA Compliance Officer or, if he is unavailable, Bret Carroll, Chief Financial Officer.

**3. Responsibilities of CALEA Compliance Officer.** The CALEA Compliance Officer shall determine if there is appropriate legal authorization for the interception of communications or access to CII.

- A. Appropriate legal authorization.** Conway Corporation's CALEA Compliance Officer shall not allow government entities to intercept communications or to access call-identifying information without appropriate legal authorization, as specified in Exhibit 1.

For requests other than those detailed in Exhibit 1, the CALEA Compliance Officer shall contact legal counsel to determine if appropriate legal authorization exists.

- B. Authorization form.** Where appropriate legal authorization exists, the Compliance Officer shall authorize appropriate personnel to intercept communications or provide call-identifying information on the Authorization and Certification Form attached as Exhibit 2.
- C. Emergency interception form.** Where a law enforcement officer requests an emergency interception, the CALEA Compliance Officer shall also complete the emergency interception form attached as Exhibit 3.
- D. Questions regarding legal authorization.** If the CALEA Compliance Officer is unable to determine whether appropriate legal authorization exists, he shall contact legal counsel for assistance.
- E. Report unauthorized acts.** The CALEA Compliance Officer shall report to affected law enforcement agencies, within a reasonable time, any unauthorized access to a lawful interception, or any act of unlawful electronic surveillance on Conway Corporation's premises, and shall fill out the Unauthorized Interception/Access/Surveillance Form attached as Exhibit 4.
- F. Maintain records of interceptions.** Conway Corporation's CALEA Compliance Officer shall be responsible for maintaining records of interceptions for a period of 5 years on the Authorization and Certification Form attached as Exhibit 2. The Form shall be compiled within a reasonable period of time after the interception and shall include the following information:
- The telephone number, circuit ID number, IP address, etc. involved;
  - The start date and time that the carrier enables the interception;

- The identity of the law enforcement officer presenting the authorization;
- The name of the person signing the authorization;
- The type of interception (for example, pen register, trap and trace etc.); and
- The name of the compliance officer
- The signature of the compliance officer, with a certification the record is complete and accurate.
- The legal authorization and any extensions that have been granted.

**G. Maintain a copy of this Plan.** The CALEA Compliance Officer shall maintain a copy of this Plan and shall be familiar with these procedures.

**H. Resubmission to FCC.** In the event that Conway Corporation (i) revises this Plan; (ii) merges with any other entity, or (iii) divests its interest in any other entity, the CALEA Compliance Officer shall resubmit this Plan to the FCC within 90 days of modification, merger or divestiture.

**Exhibit 1**  
**Legal Authorization for Broadband-Related Information<sup>1</sup>**

Surveillance Requested	Minimum Authority Necessary for LEA Access	Exceptions where authority is not necessary	Limitations on authority
<p><b>Pen register or trap and trace device (i.e. source and destination information)</b></p>	<p><b>Court Order</b></p> <p>The order must specify:</p> <ol style="list-style-type: none"> <li>1. The identity (if known) of the customer;</li> <li>2. The identity (if known) of the subject of the investigation;</li> <li>3. The phone number or other identifier and the location where the device is to be attached;</li> <li>4. In the case of a state LEA, the geographic limits of the order;</li> <li>5. The offense to which the request relates.</li> </ol>	<ol style="list-style-type: none"> <li>1. Where the LEA reasonably determines that (A) an <b>emergency situation</b> exists that involves (i) immediate danger or death or serious bodily injury; (ii) conspiratorial activities characteristic of organized crime; (iii) an immediate threat to national security; or (iv) an ongoing attack on a protected computer; (B) there are grounds for the issuance a court order, but the situation requires interception before one can be obtained.</li> <li>2. Where the customer consents.</li> </ol>	<ol style="list-style-type: none"> <li>1. The LEA must use technology reasonably available to restrict the recording or decoding to routing and addressing information (i.e., the contents of the transmission cannot be intercepted).</li> <li>2. The order cannot exceed 60 days (but the LEA can obtain extensions).</li> </ol>
<p><b>Interception of message content (for communication in transit)</b></p>	<p><b>Court Order</b></p> <p>The order must specify:</p> <ol style="list-style-type: none"> <li>1. The identity (if known) of the customer;</li> <li>2. The facilities where authority to intercept is granted;</li> <li>3. The type of communication sought;</li> <li>4. The offense to which the interception relates;</li> <li>5. The identity of LEA;</li> <li>6. The judge or magistrate authorizing the interception;</li> <li>7. The period during which the interception is authorized, and whether or not the interception terminates when the communication is obtained.</li> </ol>	<ol style="list-style-type: none"> <li>1. Where the LEA reasonably determines that (A) an <b>emergency situation</b> exists that involves (i) immediate danger or death or serious bodily injury; (ii) conspiratorial activities characteristic of organized crime; or (iii) conspiratorial activities threatening national security; and (B) there are grounds for the issuance a court order, but the situation requires interception before one can be obtained.</li> <li>2. Where one party to the communication consents.</li> </ol>	<ol style="list-style-type: none"> <li>1. The order cannot exceed 30 days (but the LEA can obtain extensions). The 30-day period begins on the earlier of the day the interception begins, or 10 days after the order is entered.</li> <li>2. In an emergency situation, the LEA must apply for an order within 48 hours.</li> </ol>

<sup>1</sup> Note that different requirements apply to real-time interception of communications in transit than to accessing stored communications.

Surveillance Requested	Minimum Authority Necessary for LEA Access	Exceptions where authority is not necessary	Limitations on authority
<p><b>Interception of contents of communication (for example, email) electronically <u>stored</u> for 180 days or fewer</b></p>	<p><b>Warrant</b></p>	<ol style="list-style-type: none"> <li>1. When the originator or addressee consents to the disclosure.</li> <li>2. If the contents were (i) inadvertently obtained by Conway Corporation, and (ii) appear to pertain to the commission of a crime.</li> <li>3. If Conway Corporation believes, in good faith, that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay.</li> </ol>	
<p><b>Interception of contents of communication (for example, email) electronically <u>stored</u> for more than 180 days</b></p>	<p><b>Warrant, or, <u>if prior notice is given to the subscriber</u>, a court order or administrative subpoena</b></p>	<ol style="list-style-type: none"> <li>1. When the originator or addressee consents to the disclosure.</li> <li>2. If the contents were (i) inadvertently obtained by Conway Corporation, and (ii) appear to pertain to the commission of a crime.</li> <li>3. If Conway Corporation believes, in good faith, that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay.</li> </ol>	
<p><b>Basic customer information</b></p>	<p><b>Administrative or trial subpoena, warrant, or court order</b></p> <p>Records that can be released include customer name, address, records of session times and durations, length of service, types of service, network address, and means and source of payment.</p>	<ol style="list-style-type: none"> <li>1. Customer consent.</li> </ol>	

Surveillance Requested	Minimum Authority Necessary for LEA Access	Exceptions where authority is not necessary	Limitations on authority
<p><b>Basic customer information (cont'd)</b></p>	<p><b>Certification in writing from the Director of the FBI or his designee</b></p>		<ol style="list-style-type: none"> <li>1. Limited to records showing name, address, length of service, and local or long distance toll billing.</li> <li>2. Records can be obtained only where relevant to an investigation to protect against international terrorism or clandestine intelligence activities</li> </ol>
<p><b>Other customer records related to internet services</b></p>	<p><b>Warrant or court order</b></p>	<ol style="list-style-type: none"> <li>1. When the subscriber consents to the disclosure.</li> <li>2. If Conway Corporation believes, in good faith, that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay.</li> </ol>	

**EXHIBIT 2**

**AUTHORIZATION AND CERTIFICATION FORM**

I certify that the attached law enforcement request for interception of (check appropriate box(es)):

- Interception of communications
- Access to call-identifying information

is based on both appropriate legal authorization and appropriate carrier authorization, as those terms are defined in Conway Corporation's Systems Security and Integrity Plan, and, based on these authorizations, the interception/access should be enabled.

**ATTACH A COPY OF THE COURT ORDER OR OTHER WRITTEN AUTHORIZATION THAT IS THE BASIS OF LEGAL AUTHORIZATION.**

Telephone numbers and circuit identification numbers involved: \_\_\_\_\_

Start date and time of the interception: \_\_\_\_\_

Identity of law enforcement personnel: \_\_\_\_\_

Name of person authorizing interception/access: \_\_\_\_\_

Type of interception or access to call-identifying information: \_\_\_\_\_

I certify that the above information is complete and accurate to the best of my knowledge.

\_\_\_\_\_  
Signature of CALEA Compliance Officer

\_\_\_\_\_  
Print Name

\_\_\_\_\_  
Date

**EXHIBIT 3**

**EMERGENCY INTERCEPTION FORM**

Name of Officer: \_\_\_\_\_

Badge or ID number: \_\_\_\_\_

Position: \_\_\_\_\_

Law Enforcement Agency: \_\_\_\_\_

Interception requested:

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

I certify that the above-referenced Officer has confirmed to me that an emergency situation exists that involves:

- (i) immediate danger of death or serious physical injury;
- (ii) conspiratorial activities threatening the national security interest;
- (iii) conspiratorial activities characteristic of organized crime; or
- (iv) an ongoing attack on a protected computer

and that there are grounds upon which an order could be entered authorizing this interception, however, interception is required before an order could, with due diligence, be obtained.

\_\_\_\_\_  
Signature of CALEA Compliance Officer

\_\_\_\_\_  
Print Name

\_\_\_\_\_  
Date

**EXHIBIT 4  
Unauthorized Acts**

**UNAUTHORIZED INTERCEPTION/ACCESS/SURVEILLANCE FORM**

The following incident occurred involving (check one)

Unlawful interception of communications or access to call-identifying information

Unlawful electronic surveillance on Conway Corporation's premises

[describe] \_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_  
Signature of CALEA Compliance  
Officer

\_\_\_\_\_  
Print Name

\_\_\_\_\_  
Date

## **APPENDIX 1**

### **Conway Corporation's CALEA Compliance Officer: Roy Grubb**

Conway Corporation's CALEA Compliance Officer is responsible for ensuring that any interception of communications or access to call-identifying information that takes place Conway Corporation's premises be activated only in accordance with a court order or other lawful authorization. The Compliance Officer is also responsible for reporting any unauthorized surveillance or disclosures of call-identifying information to appropriate law enforcement personnel, and is responsible for maintaining records of any interceptions.

### **The Compliance Officer may be contacted at the following telephone numbers:**

Name: Roy Grubb

Title: Administrator, Broadband Services

Work Phone: (501) 450-6098

Cell Phone: (501) 472-3622

### **In the event that the Compliance Officer is unavailable, please contact:**

Name: Jason Hansen

Title: Chief Technology Officer

Work Phone: (501) 450-6011

Cell Phone: (501) 733-0025