

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

**EB Docket 06-36**

Annual 64.2009(e) CPNI Certification for 2012

Date filed: February 28, 2014

Name of company covered by this certification: Cisco WebEx LLC

Form 499 Filer ID: 826750

Name of signatory: William Hodkowski

Title of signatory: Vice President & Assistant Secretary

I, William Hodkowski, 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 (including those mandating the adoption of CPNI procedures, training, recordkeeping, and supervisory review) set forth in section 64.2001 *et seq.* of the Commission's rules.

The company has not taken any actions (*i.e.*, proceedings instituted or petitions filed by the company at either state commissions, the court system, or at the Commission against data brokers) during the period covered by this certification.

The company has not received any customer complaints during the period covered by this certification concerning the unauthorized release of CPNI.

The company represents and warrants that the above certification is consistent with 47 C.F.R. § 1.17, which requires truthful and accurate statements to the Commission. The company also acknowledges that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may subject it to enforcement action.

Signed   
William Hodkowski

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

**EB Docket 06-36**

**Attachment 1: Statement Concerning Company Procedures**

**General duty, training, and discipline.**

Cisco WebEx LLC (the “Company”) has adopted and distributed to all employees a Customer Proprietary Network Information Standard (“CPNI Policy”) that addresses proper handling and use of CPNI and advises all employees of their duty to safeguard CPNI. Employees are advised that violations of the CPNI Policy will subject an employee to disciplinary action, up to and including immediate termination of employment. The Company makes CPNI available to employees only on a need-to-know basis.

**Use of customer proprietary network information without customer approval (47 C.F.R. § 64.2005); Approval required for use of customer proprietary network information (47 C.F.R. § 64.2007); Notice required for use of customer proprietary network information (47 C.F.R. § 64.2008); Safeguards required for use of customer proprietary network information (47 C.F.R. § 64.2009)**

The Company does not use, disclose, or permit access to CPNI for marketing purposes except as permitted by Section 222 of the Communications Act or regulations implementing Section 222 of the Communications Act. The Company does not disclose CPNI to third parties or permit third parties to access or use CPNI, except as permitted by Section 222 of the Communications Act or regulations implementing Section 222 of the Communications Act.

**Safeguards on the disclosure of customer proprietary network information (47 C.F.R. § 64.2010)**

The Company does not provide any in-store access to CPNI.

The Company does not provide any telephone access to call detail information based on customer-initiated telephone contact. Customers requesting call detail information by telephone will be provided with call detail information only by sending it to the customer’s address of record. If a customer is able to provide call detail information to the Company during a customer-initiated call without the Company’s assistance, the Company will discuss the call detail information provided by the customer.

Customers may access their CPNI online and establish a password for future access only after they have been authenticated without using readily available biographical information or account information. After initial authentication, customers may only access CPNI online by providing a password that is not prompted by a request for readily available biographical information or account information. If a customer cannot provide

the correct password, the customer must be reauthenticated before being provided with a password.

The Company notifies customers immediately by email to the customer's email address of record or by mail to the customer's postal address of record of any changes to a lost or forgotten customer password, online account information, or address of record. This notice does not reveal the changed information and is sent to the existing address, not to an address that has been changed.

**Notification of customer proprietary information security breaches (47 C.F.R. § 64.2011)**

The Company's operating procedures require notification of relevant law enforcement agencies and customers in accordance with FCC rules in the event of a breach of CPNI. The Company maintains records of any breaches discovered, notifications made to law enforcement, and notifications made to customers. These records include, where available, dates of discovery and notification, a detailed description of the CPNI that was the subject of the breach, and the circumstances of the breach. The Company retains these records for 2 years.