UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
TYLER DIVISION

NETWORK-1 SECURITY SOLUTIONS, INC., Plaintiff, v. CISCO SYSTEMS, INC., CISCO-LINKSYS LLC, ADTRAN, INC., ENTERASYS NETWORKS, INC., EXTREME NETWORKS, INC., FOUNDRY NETWORKS, INC., NETGEAR, INC., and 3COM CORPORATION, Defendants.	CIVIL ACTION NO. 6:08 CV 30 PATENT CASE

STIPULATED PROTECTIVE ORDER

This protective order ("Protective Order") is issued to expedite the flow of discovery materials, to facilitate the prompt resolution of disputes over confidentiality of discovery materials, to adequately protect information the parties are entitled to keep confidential, to ensure that only materials the parties are entitled to keep confidential are subject to such treatment, and to ensure that the parties are permitted reasonably necessary uses of such materials in preparation for and in the conduct of trial, pursuant to Fed. R. Civ. P. 26(c) and any other applicable rule of this Court. Unless modified, superseded or terminated pursuant to the terms contained in this Order, this Protective Order shall remain in effect through the conclusion of this litigation and thereafter as set forth below.

AVAYA INC. AV-1020

In support of this Protective Order, the Court finds that:

1. Documents or information containing confidential research, development, business and/or commercial information and/or trade secrets within the meaning of Rule 26(c) ("Confidential Information") is likely to be disclosed or produced during the course of discovery in this litigation;

2. The parties to this litigation may assert that public dissemination and disclosure of Confidential Information could severely injure or damage the party disclosing or producing the Confidential Information and/or could place that party at a competitive disadvantage;

3. Counsel for the party or parties receiving Confidential Information are presently without sufficient information to accept the representation(s) made by the party or parties producing Confidential Information as to the confidential, proprietary, and/or trade secret nature of such Confidential Information; and

4. To protect the respective interests of the parties and to facilitate the progress of disclosure and discovery in this case, the following Protective Order should issue.

IT IS THEREFORE ORDERED THAT:

1. This Protective Order shall apply to all information, documents and things subject to discovery in this Action produced either by a party or a non-party in discovery in this Action ("Action" shall include without limitation this litigation and any adjunct subpoena proceedings incident hereto before any tribunal) including, without limitation, testimony adduced at deposition upon oral examination or upon written questions, answers to interrogatories, documents and things produced, information obtained from inspection of premises or things, and answers to requests for admission, or information disclosed pursuant to subpoena under Fed. R. Civ. P. 45 ("Discovery Material").

2. Each party to this litigation that produces or discloses any materials, answers to

interrogatories, responses to requests for admission, trial testimony, deposition testimony, and transcripts of trial testimony and depositions, or information that the producing party believes should be subject to this Protective Order may designate the same as "CONFIDENTIAL," "HIGHLY CONFIDENTIAL – OUTSIDE COUNSEL ONLY," or "HIGHLY CONFIDENTIAL – RESTRICTED SOURCE CODE (referred to collectively as "Confidential Material"). The producing party may use the designation "HIGHLY CONFIDENTIAL – RESTRICTED SOURCE CODE" to designate computer source code or documents that describe algorithms used in computer source code. Confidential Materials designated as "HIGHLY CONFIDENTIAL – OUTSIDE COUNSEL ONLY" or "HIGHLY CONFIDENTIAL – RESTRICTED SOURCE CODE" are hereinafter collectively referred to as "HIGHLY CONFIDENTIAL" material.

a. Designation as "CONFIDENTIAL": The term "CONFIDENTIAL" information shall apply to a party's confidential and nonpublic information, the disclosure of which the Disclosing Party contends could cause harm to the business operations of the Disclosing Party or provide improper advantage to others, and that is not otherwise marked or designated by the Disclosing Party as "HIGHLY CONFIDENTIAL – OUTSIDE COUNSEL ONLY," or as "HIGHLY CONFIDENTIAL – RESTRICTED SOURCE CODE."

b. Designation as "HIGHLY CONFIDENTIAL – OUTSIDE COUNSEL ONLY": The term "HIGHLY CONFIDENTIAL – OUTSIDE COUNSEL ONLY" shall apply only to a party's highly confidential and proprietary business, commercial, competitive, financial, marketing, sales and technical information that the Disclosing Party reasonably and in good faith believes is so highly sensitive that its disclosure to an employee of a Discovering Party would reveal significant business, commercial, competitive, financial, marketing, sales or technical advantages of the Disclosing Party. The term "HIGHLY CONFIDENTIAL –

OUTSIDE COUNSEL ONLY" information shall include, but is not limited to, (1) current business/strategic plans, (2) sales, cost and price information including future sales/financial projections, (3) non-public marketing information including future marketing plans, (4) detailed sales and financial data that includes costs and profits information, (5) customer lists, (6) licensing, licensing policies, and licensing negotiations, (7) non-public source code, specifications, schematics and other documents used in connection with generating such source code, and other non-public technical specifications, schematics and documents showing the Disclosing Party's product functionality, features and operation and (8) other information of business, commercial, competitive, financial, marketing, sales and technical significance comparable to the items listed in this paragraph. For purposes of this Order, the term "source code" shall include human-readable and machine-readable program codes, as well as executable code and electronically created design files such as CAD files.

3. In determining the scope of information which a party may designate as its Confidential Material, each party acknowledges the importance of client access to information necessary to client decision-making in the prosecution or defense of litigation, and therefore agrees that designations of information as Confidential Material and responses to requests to permit further disclosure of Confidential Material shall be made in good faith and not (1) to impose burden or delay on an opposing party or (2) for tactical or other advantage in litigation. No published documents shall be designated as CONFIDENTIAL or HIGHLY CONFIDENTIAL, even if the published documents are attachments to, or intermingled with, documents properly designated as CONFIDENTIAL or HIGHLY CONFIDENTIAL.

4. The labeling or marking of a document or tangible thing with the designation "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL" shall be made when a copy of the document or thing is provided to the receiving party by placing the legend "CONFIDENTIAL,"

"HIGHLY CONFIDENTIAL – OUTSIDE COUNSEL ONLY," or "HIGHLY CONFIDENTIAL – RESTRICTED SOURCE CODE" on the face of each such document or thing. Any such designation that is inadvertently omitted or misdesignated may be corrected by written notification to counsel for the receiving party, and the receiving party shall thereafter mark and treat the materials as "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL," as appropriate, and such material shall be subject to this Protective Order as if it had been initially so designated. If, prior to receiving such notice, the receiving party has disseminated the Confidential Material to individuals not authorized to receive it hereunder, it shall make a reasonable effort to retrieve the Confidential Material or to otherwise assure that the recipient(s) properly mark the Confidential Material and maintain the confidentiality of the Confidential Material, but shall have no other responsibility or obligation with respect to the information disseminated.

5. In the case of deposition upon oral examination or written questions, such testimony shall be deemed "CONFIDENTIAL" until the expiration of thirty (30) days after the deposition unless otherwise designated at the time of the deposition or during the thirty (30) day period. Pages or entire transcripts of testimony given at a deposition or hearing may be designated as containing "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL" information by an appropriate statement either at the time of the giving of such testimony or by written notification within thirty (30) days after the deposition. If the testimony is not otherwise designated at the time of the deposition or during the thirty (30) day period after the deposition, the testimony will be deemed to be "non-confidential." Within 15 days of the delivery of the transcript of any such deposition or hearing, any person who designated information in the transcript as CONFIDENTIAL or HIGHLY CONFIDENTIAL shall serve a first redacted version that omits only such HIGHLY CONFIDENTIAL materials, so that persons with CONFIDENTIAL information access may review the remainder of the discovery responses, and

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.