**IN THE UNITED STATES DISTRICT COURT**
**FOR THE EASTERN DISTRICT OF TEXAS**
**TEXARKANA DIVISION**

| | | |
|---|---|---|
| **ESN, LLC,** | ) | |
| | ) | |
| **Plaintiff,** | ) | |
| | ) | |
| | ) | |
| **v.** | ) | **Civil Action No. 5:08-CV-20-DF** |
| | ) | |
| **CISCO SYSTEMS, INC., and**<br>**CISCO-LINKSYS, LLC,** | ) | |
| | ) | |
| | ) | |
| **Defendants.** | ) | |

## JOINT MOTION FOR ENTRY OF A PROTECTIVE ORDER

Plaintiff ESN, LLC ("ESN") and Defendants Cisco Systems, Inc. and Cisco-Linksys, LLC (collectively "Cisco") hereby jointly submit the attached Protective Order. However, despite numerous conversations and numerous different proposals, ESN and Cisco have one remaining provision that they could not agree upon. The provision at issue is in paragraph 14(d)(i) and specifically relates to the number of pages of Computer Source Code (which is required to be reviewed by the receiving party on a standalone computer maintained in the possession of the production party) that the receiving party is allowed to print.

ESN has proposed the following language for paragraph 14(d)(i):

> A laser printer with an adequate paper supply shall be attached to the Standalone Computers and the receiving party shall only make hard copies of HIGHLY RESTRICTED CONFIDENTIAL material that they in good faith consider to be necessary to proving the elements of their case. If the producing party believes that the receiving party is abusing this provision, the producing party may seek relief from the Court, for example, to limit the total number of pages printed by the receiving party.

Cisco has proposed the following language for paragraph 14(d)(i):

> A laser printer with an adequate paper supply shall be attached to the Standalone Computers and the receiving party shall make no more than 500 total pages of

> hard copies of HIGHLY RESTRICTED CONFIDENTIAL material that they in good faith consider to be necessary to proving the elements of their case. The number of total pages of hard copies of HIGHLY RESTRICTED CONFIDENTIAL material that the receiving party may in good faith make may be expanded upon a showing of good cause.

**<u>ESN's Position</u>**

ESN cannot agree to a hard limit on the number of Computer Source Code pages that it may print when it has no way of knowing the nature and volume of the relevant Computer Source Code that will be necessary to prove the elements of its case. ESN further believes that the 500-page limitation is arbitrary and unnecessary in light of the numerous other protections set forth in the Protective Order that ESN has already agreed to, which restrict the location and manner in which Computer Source Code can be reviewed, and insulates the Computer Source Code from disclosure to anyone other than retained experts and trial counsel that have previously been disclosed to Cisco. ESN's proposal also allows Cisco to seek further relief if it believes ESN is abusing its printing privileges. The Computer Source Code provisions of the proposed Protective Order already agreed to by ESN are onerous enough and would become unduly so if the page limit proposed by Cisco is adopted by the Court. Further, Cisco's proposal would require the Court to micromanage the issue of determining what source code is relevant.

ESN had proposed a compromise whereby ESN would only be allowed to have up to 3000 printed pages of Computer Source Code in its possession at any given time, but would be allowed to return copies and receive a page-for-page credit toward additional pages. This would eliminate Cisco's concern that ESN could possess an unlimited number of printed pages of Computer Source Code, but would allow ESN to turn back in pages that it determines after further analysis are less relevant than other pages that it needs to prove its case. This also would have eliminated Cisco's ability to unilaterally determine whether ESN needs additional or alternative printed pages. Cisco rejected ESN's proposed compromise.

**<u>Cisco's Position</u>**

### I. The Importance of Protecting Cisco's Source Code.

The security of Cisco's systems, and the systems of its customers, partners, and many of the world's Internet users, depends on the confidentiality of the source code associated with Cisco's products. If any portion of the source code for the operating systems of Cisco's products are made public, not only could Cisco suffer considerable financial damage and loss of sales from unauthorized use and copying of the code, but the potential for persons to misuse the code to hack into Cisco operating systems would create significant security problems for Cisco and for Cisco's many customers throughout the world.

Cisco's customers include the U. S. Government and many major public institutions and private corporations. Cisco products are used by many security conscious agencies of the Federal government and Cisco provides special training on its products to enable Federal systems administrators to maintain the security of information handled by Federal agencies. Accordingly, our nations' security is also implicated by the potential disclosure of Cisco's confidential source code.

Once the source code, or any portion there of, is compromised, there is no easy way to repair the resulting damage to Cisco and the varied users of its products. Because much of Cisco's IOS[1] code is highly integrated, if even portions of Cisco's source code is inadvertently or otherwise disclosed to a third party or made public, the probability of a hacker penetrating Cisco's security measures increases dramatically. The source code could be used by a hacker or

[1] Cisco's IOS is the software used on the majority of Cisco's routers.

an unauthorized user as a “road map” to enable them to breach the security measures built into the products and thus gain access to the information and data being processed and transmitted by the Cisco products.

## II. Cisco’s Efforts to Preserve the Confidentiality of Its Source Code.

Given the critical importance of protecting its source code, Cisco has employed a number of different security systems and procedures to protect the confidentiality of its source code. These security measures include extra security steps that may not be required for other types of confidential information. As a first measure of security, for example, Cisco requires employees who may have access to its confidential materials to undergo a thorough background check and agree to abide by a strict confidentiality agreement. Employees are also expected to adhere to Cisco’s code of business conduct, which requires the protection of the confidential and proprietary information of Cisco and its customers, including Cisco’s source code. Access to Cisco’s facilities also is restricted, as Cisco’s policies provide for security badges access for employees and registration and escort of guests.

Cisco’s security policies and practices limit access to its source code only to certain employees, and even then on a restricted basis. Access to the source code is limited to the minimum amount of access that is reasonably necessary for an employee to perform his or her duties. Generally, a software engineer with access to an image of the IOS source code does not have sufficient permission to access all of the IOS source code.

Cisco also employs security measures with respect to how and where source code is accessed. In order for an individual to view the source code, the user must access Cisco’s systems with appropriate login credentials from an approved location within Cisco’s corporate network, which is guarded from the outside Internet by firewalls and intrusion prevention systems. Prior to granting access to the source code, Cisco's data center verifies a user's login credentials and the physical address of the computer from which the user is accessing the data center.

### III. Cisco's Proposal Does Not Interfere With ESN's Need For Information To Prosecute Its Claim.

Cisco's proposed protections are reasonable to prevent the real harm that could result from unauthorized disclosure or use of the source code. Indeed, ESN agrees that source code is entitled to more protection than other types of confidential information. Cisco's proposal guarantees this additional protection, while still providing ESN with information that may be necessary to prosecute its infringement claims against Cisco.

ESN cannot and does not contend that Cisco's proposal interferes with its need for certain information. Rather, ESN merely argues that it may need to print more than 500 pages of source code to prove its case. ESN's argument fails for two reasons. First, it is speculative. ESN has offered no reason to believe that it will need to print more than 500 pages of source code. Second, even if ESN does require more than 500 pages of source code, it will be permitted to print those pages upon a showing of good cause. While Cisco's protocol does provide printing restrictions (Cisco would, of course, operate under the same restriction while reviewing ESN's source code), the restrictions are minor given the relative security concerns associated with the source code.

In fact, Cisco's proposed printing restrictions are not unique. This Court has ordered similar 500 page limits on source code printing in *QPSX Developments 5 Pty Ltd. v. Juniper Networks, Inc., et al.,* 2-05-CV-268-TJW (E.D. Tex.) (*see* DN 103 ¶ 11(j)), a case in which Cisco's source code was at issue, and *Reid v. General Motors Corp.*, 2:05-CV-401-TJW (E.D.

Tex.) (*see* DN 56 ¶ 6(j).) Cisco merely requests printing restrictions that this Court has previously ordered under similar circumstances.

Despite the best efforts of counsel for the respective parties, they are at an impasse on this issue. Therefore, the parties respectfully submit this issue to the Court, and request that the Court decide which provision should be included in the Protective Order.

Respectfully submitted,

FOR PLAINTIFF, ESN, LLC:

EMAlbritton

Eric M. Albritton
Lead Attorney
Texas State Bar No. 00790215
ALBRITTON LAW FIRM
P.O. Box 2649
Longview, Texas 75606
Telephone (903) 757-8449
Facsimile (903) 758-7397
ema@emafirm.com

T. John Ward Jr.
Texas State Bar No. 00794818
Ward & Smith Law Firm
111 W. Tyler St.
Longview, Texas 75601
Telephone (903) 757-6400
Facsimile (903) 757-2323
jw@jwfirm.com

George P. McAndrews
Thomas J. Wimbiscus
Peter J. McAndrews
Gerald C. Willis
McAndrews, Held & Malloy, Ltd.
500 W. Madison Street, 34th Floor
Chicago, Illinois 60661
Telephone (312) 775-8000
Facsimile (312) 775-8100
pmcandrews@mcandrews-ip.com

FOR DEFENDANTS CISCO SYSTEMS, INC.
AND CISCO-LINKSYS, LLC

/s/ Victoria F. Maroulis by permission
Sam Baxter
McKool Smith, P.C.
104 E. Houston Street, Suite 300
P.O. Box 0
Marshall, Texas 75670
sbaxter@mckoolsmith.com

Garrett W. Chambers
McKool Smith, P.C.
300 Crescent Court, Suite 1500
Dallas, Texas 75201
gchambers@mckoolsmith.com

Charles K Verhoeven
Quinn Emanuel Urquhart Oliver & Hedges, LLP
50 California St., 22nd Floor
San Francisco, CA 94111
charlesverhoeven@quinnemanuel.com

Victoria F. Maroulis
Quinn Emanuel Urquhart Oliver & Hedges, LLP
555 Twin Dolphin Dr., Suite 560
Redwood Shores, CA 94065
victoriamaroulis@quinnemanuel.com

## CERTIFICATE OF SERVICE

The undersigned certifies that the foregoing document was filed electronically in compliance with Local Rule CV-5(a). As such, this motion was served on all counsel who are deemed to have consented to electronic service. Local Rule CV-5(a)(3)(A). Pursuant to Fed. R. Civ. P. 5(d) and Local Rule CV-5(d) and (e), all other counsel of record not deemed to have consented to electronic service were served with a true and correct copy of the foregoing by email and/or fax, on this the 28th day of May, 2008.

EMAlbritton

Eric M. Albritton