



Cisco Systems, Inc.
170 W. Tasman Drive
San Jose CA 95134-1706
<http://www.cisco.com>

September 30, 2004

Secretary,
Federal Trade Commission
Room 159-H (Annex V)
600 Pennsylvania Avenue NW
Washington, DC 20580

Re: Email Authentication Summit-Comments, (Matter Number P044411)

Dear Mr. Secretary:

Cisco Systems, Inc. ("Cisco") is pleased to respond to the Federal Trade Commission's (the "Commission") and the National Institute of Standards and Technology's ("NIST") Request for Comments in connection with the planned Email Authentication Summit of November 9-10, 2004. Spam is an important issue, and the Commission's decision to sponsor an Authentication Summit provides a useful public service which will increase the understanding of the role authentication can play in reducing spam.

In October of 2003, Cisco decided to work on a technological approach to spam. We developed the Identified Internet Mail authentication framework, and are currently advancing it through the Internet Engineering Task Force ("IETF"). Cisco undertook this work because of the growing cost of spam to email users generally, to Cisco's customers, and to Cisco itself. An effective authentication system should give users and system administrators the ability to choose features which will reduce the requirement for multi-layered filtering and excess storage, improve latency, and allow more flexibility and choice regarding email.

Spam is often sent using techniques designed to disguise the true source of the message. This typically prevents attempts to shut down the spammer. In some cases, spammers can also disguise the identity of infected systems sending messages. Since the Simple Mail Transfer Protocol ("SMTP") permits senders to use any return address they wish, an authentication system that includes the addition of a cryptographic signature to a message will limit the opportunity of spammers or malware (worms, viruses, etc.) to forge return addresses, and thus provides a degree of accountability for the source of email messages.

Cisco's signature-based authentication proposal, Identified Internet Mail, describes backward-compatible extensions to the format of email, and a public-key infrastructure to permit verification of the source of messages by either mail transfer agents (MTAs) or mail user agents (MUAs). This proposal is flexible in that the required changes are

