Dear Member of the Media or Analyst Community:

It has come to our attention that you may have received information about NeoScale and the December 18th, 2006 CERT report. You may be aware that CERT, the official organization that collects and manages computer security threats, published a reported 'vulnerability' in the NeoScale CryptoStor Tape 700 products. This advisory also contained NeoScale's response that states that the issue called out in the report relates to legacy versions of the NeoScale product, and has been addressed for shipping products. NeoScale has also made product upgrades available to our customers at no additional charge.

I'd like to provide a little context behind this reported vulnerability so that you can fully understand its potential impact. CERT categorizes reported vulnerabilities according to a 'Severity Metric' that ranges from 0 (low) to 180 (high). This reported vulnerability was rated at 0.64 (zero point six four). And as you may know, there are many leading companies who have hundreds of CERT advisories posted. That being said, we take any vulnerability very seriously as data security is our mission. NeoScale regularly tests the security of our products using internal and external sources to find vulnerabilities proactively. When problems are discovered, NeoScale works to resolve these problems and make them available to our customer base as described in the NeoScale Security Policy.

CERT characterized this vulnerability as one that could allow a malicious user to bypass additional two factor authentication ***if*** they had knowledge of a security officer's user ID and password. Neoscale has fully addressed this reported vulnerability in v2.6 of the CryptoStor Tape Appliance code -- available on all NeoScale CryptoStor Tape 700 Appliances. This resolution addresses both the vulnerability itself as well as any possible residual effects from an old ActiveX control remaining on the browser platform.

NeoScale has been informed that NetApp/Decru generated an email to customers, partners, and the press in a negatively-oriented marketing campaign which states 'An attacker who obtains a user password can "gain access to the System Key" without presenting a smartcard.' This statement is completely false, is not included anywhere in the CERT advisory VU #339004, and has nothing whatsoever to do with the CERT advisory. We're disappointed this misinformation was widely distributed in an attempt to mis-characterize and deposition NeoScale -- and we are happy to set the record straight.

As 2006 draws to a close, we'd like to emphasize that this was a banner year for NeoScale:

- The U.S. National Institute of Standards and Technology (NIST) awarded FIPS 140-2 Level 3 Certificate #621 to NeoScale's CryptoStor Tape 702/704, the first tape security appliance to achieve this certification level. With this certification, NeoScale delivers Pentagon-class information security to government agencies, exceeding regulatory compliance standards related to secure IT environments.
- CryptoStor KeyVault™ was unveiled as the industry's first open security key management system to deliver centralized management of both NeoScale encryption appliance keys and those from third-party storage encryption vendors.
- We launched the industry's first tape security appliance to support native 4-Gbps interfaces, the CryptoStor Tape 712. It allows customers to double the number of tape drives secured on a single channel.

If you would like to know more, we would be happy to speak with you.

Sincerely,

Barbara Nelson
CEO, NeoScale