Procedural Addendum to
NSHE Spam and Virus Policy

History

During the previous years in which spam policy was discussed, a dramatic change in the E-mail landscape has occurred. Estimates show bulk, unwanted E-mail accounting for 80-90 percent of all electronic messages being processed. The phenomenal growth in E-mail use on Fallon and Pioneer E-mail systems has also created the same level of growth in spam. This has caused significant performance and service degradation issues which require attention. The policy change reflects best practices and is consistent with spam filtering policies in wide use at NSHE institutions already.

Goal

The policy changes have been designed to deal with the evolving landscape of E-mail services and threats associated with the large volumes of unsolicited, unwanted bulk E-mail. Specific goals of the policy change are to:

- Implement industry standard best practices
- Improve performance and service levels for E-mail users
- Reduce the unchecked threat of phishing attacks which could result in identity theft
- Reduce and/or eliminate the continuous black listing of NSHE E-mail domains caused by the previous policy and dramatic increase in spam.
- Allow flexibility in solutions that comply with policy and NSHE goals

Procedure

Mail originating from a network address listed in the Domain Name Service Blackhole Lists (DNSbls) will be rejected. No notification will be sent by SCS to the intended recipient. Computer generated notification is typically sent to the sender per RFC standards.

Flexible open source and commercial spam filtering solutions will be deployed that follow an acknowledged spam scoring system. Thresholds for spam to be rejected will be established based on industry averages and internal analysis. E-mail that scores above the adopted spam threshold will be rejected. E-mail that scores below the threshold but may still be considered spam will be tagged and forwarded with the following subject line:

[SPAM WARNING] Original text line

The threshold setting will be reviewed quarterly and adjustments will be communicated to CTO's. Other spam filtering technologies may be deployed as appropriate to accommodate detection-avoidance techniques and meet the stated goals.

E-mail will be scanned for viruses. Attachments determined to be viral will be rejected.

Potentially dangerous executable attachments including but not limited to (.ade, .adp, .bas, .bat, .chm, .cmd, .com, .cpl, .crt, .exe, .hlp, .hta, .inf, .ins, .isp, .js, .jse, .mdb, .mde, .msc, .msi, .msp, .mst, .pcd, .pif, .reg, .scr, .sct, .shb, .shs, .vb, .vbe, .vbs, .wsc, .wsf, and .wsh) and encrypted ZIP attachments containing such files will be rejected. All other attachments passing virus scanning will be delivered normally.

SCS Procedural Information
Revision History:

- *Version 1 - Authorized and applied 3/23/06*
- *Version 2 – Changes to spam filtering, authorized and applied 2/12/07*