Conclusion

This document has presented a discussion of the security issues involved with deploying a site H.323 videoconferencing service. While many sites may see their H.323 videoconferencing facilities function perfectly well without giving much, if any, consideration to security, security is invariably only as good as the weakest link. Thus it is important that any site involved in a videoconferencing session applies best security practice, as described by the JANET CERT team [JCERT], just as it would do for all other IP-connected devices.

However, while there are many security measures that could be taken to protect an H.323 service, the reader should bear in mind the measures taken in comparable applications such as e-mail and FTP. It is very rare for PGP encryption to be used for e-mail, and likewise most FTP users are not even aware that there is a secure counterpart (SFTP) which offers encryption (of the data, and perhaps more importantly the username and password in transit). Thus we should not expect H.323 encryption to be widely used, if at all, unless the conference subject matter is highly confidential or sensitive.

The VTAS service is available for further questions beyond this document, which itself will be revised with experience as the JVCS-IP service matures.