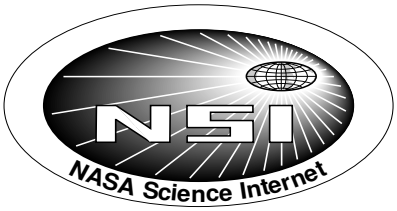

NASA Science Internet

Network Security Information

September 1993

Brad Olive,
NSI Network Security Manager

Prepared for the
NASA Science Internet Project Office
NASA Ames Research Center
By Sterling Software, Inc.
NAS2-13210-648

NASA Science Internet
Network Security Information

To: NASA Science Internet Security Contacts

From: Brad Olive
NSI Network Security Manager

Subj: NSI-CERT - Introduction

This message is intended as an introduction to the NASA Science Internet Network Security Office, and the NSI Computer Emergency Response T eam.

I am the new NSI Network Security Manager The following information has been prepared as an introduction to the NSI Network Security Office and the NSI Computer Emergency Response T eam.

The NSI Network Security Office has several mailing lists.

nsi-cert-tools : This mailing list is used to inform system and network administrators of new security tools available from the NSI Archive or from other sources.

nsi-cert-advise : This mailing list is used to contact system and network administrators of potential system vulnerabilities, patches and other important security related information.

If you would like to be on one of these lists, send e-mail with the following information to nsi-cert-info@nsipo.arc.nasa.gov

Your Name
Title
Organization
e-mail address
USMail address
Phone/Fax/Pager
Which list you want to be added to

Please indicate in your message if you are a security contact, with the machines that you have responsibiliy for . If there is an alternate emergency contact, please include that information. All initial incident contacts will be via telephone when possible.

NASA Science Internet Network Security Office

The NSI Network Security Office is located at NASA Ames Research Center to provide a source for information regarding safeguarding against network security problems, responding to incidents and providing information to systems personnel regarding security issues.

The Network Security Office will provide NSI members and affiliated groups with information on security bug-fixes, vulnerabilities and safeguards. Should an incident occur , the NSI Network Security Office will provide assistance in securing the systems and resolving the incident.

NASA Science Internet Computer Emergency Response T eam (NSI-CERT)

The NASA Science Internet Computer Emergency Response T eam (NSI-CERT) is part of the NSI Network Security Office, and was formed to work with the NASA Science Internet community to facilitate its response to computer security events involving NSI hosts, or any security events that include NSI. The NSI-CERT will also assist the NSI Community in taking proactive steps to raise security issues, and to conduct research targeted at improving the security of existing systems.

NSI-CERT provides technical assistance for responding to computer security incidents, product vulnerability assistance, and technical documents. In addition, the NSI-CERT maintains an archive that is available via the anonymous FTP server: nsipo.arc.nasa.gov where security-related documents, policies, and tools are archived.

NASA Science Internet
Security Incident Reporting Procedure

WHAT TO DO IF YOU FEEL YOUR SITE HAS HAD AN INTRUSION

If you believe that your site has experienced an intrusion, or if you have detected an intrusion, it should be reported to the NSI-CERT immediately . You should provide the NSI-CERT with as much information as possible, including opinions and thoughts as to how the breakin occurred. The NSI-CERT should be your first call.

Please use the NSI-CERT as your primary contact. The NSI-CERT will contact other agencies that need information regarding the incident. Reporting incidents and releasing information regarding a breakin to other agencies, personnel or media can have serious legal consequences if not handled properly , not to mention bad public relations. The NSI-CERT has been trained in the handling of intrusion response.

If you have access to the following information, please include it in your report:

1) names of host or hosts compromised
2) account name(s) compromised
3) architecture of compromised host(s)
4) operating system and revision of compromised host(s)
5) whether or not any security patches have been applied to the compromised host(s); if so, were patches applied before or after the intrusion
6) other host(s)/site(s) involved in the intrusion
7) if other site(s) have been contacted, the contact information used for contacting the site(s) involved
8) appropriate log extracts (including timestamps) THIS IS IMPORT ANT
9) what you have done since noticing the intrusion

If you believe that the intruder still has access to your system, avoid using e-mail to discuss the activities. Most intruders, experienced or not, look for e-mail and other files that may describe actions being taken to eradicate or trace them.

If possible, get this information directly to the Network Security Manager via fax and immediately follow up with a phone call.

NSI-CERT contact information:

Brad Olive, NSI Network Security Manager NASA Science Internet Network Security Office NASA Ames Research Center MS-233-8 Moffett Field, CA 94035-1000 U.S.A.	bolive@nsipo.arc.nasa.gov nsi-cert@nsipo.arc.nasa.gov +1 415-604-0670 voice +1 800-998-6653 message pager +1 415-604-0063 fax machine +1 415-694-9970 numeric pager

Emergency contact if unable to reach NSI Network Security at the above numbers: NSI Operations +1-800-424-9920 or +1-415-604-3655