Restricted Use of IMP DDT

    At the recent workshop on "Automated Resource Sharing on the
ARPANET", considerable interest was expressed on the topic of network
security. In particular, representatives of several sites felt that
uncontrolled use of IMP DDT made access control mechanisms quite
vulnerable to interception or tampering.* Individuals at the workshop
seemed to be in general agreement that use of DDT should be much more
controlled than at present. In addition, as the network continues to
take on a more and more operational character, and NCC use of DDT (which
must be coordinated with other DDT usage) increases** we begin to see
other reasons for controlling access to the DDT mechanism.

    Currently, and for the foreseeable future, it is important that the
NCC be able to use DDT at any IMP at any time. It is also sometimes
necessary for site personnel to be able to operate a stand alone DDT
after an IMP crash. Sometimes the NCC needs to ask site personnel to
operate the IMP DDT for the NCC if the network is partitioned. We have
protected all DDT commands that can affect the running IMP program by
requiring that sense switch 4 be turned on at the site, or a software
override flag be enabled. Only the BBN IMP Teletype, the BBN TIP
Teletype, and the PDP-1 can enable override. The NCC monitors these
flags and reports any change in status.

    In line with this approach, we will soon modify the IMP system so
that any access to IMP DDT will require the same enabling actions (sense
switch four turned on or override enabled from BBN) now required for
core modification. This will still allow the NCC the same ability to
operate DDT which it now has, and will permit site personnel to operate
DDT at the request of the NCC. As is currently true, the NCC will

----
*Examples are easy to construct, but are intentionally omitted from this
document.

**DDT is currently used by the NCC operators for core verification, for
interface debugging, for loading TIP and VDH code, etc. There is
discussion of using DDT in conjunction with an "auto-dialer" to examine
a TIP's "view" of a modem port at the same time that the auto-dialer is
examining the outside world's "view" of the port, of running "automatic"
core verification, of loading Satellite IMP code, etc.

McKenzie   [Page 1]

monitor the setting of sense switch four and take appropriate action if
unauthorized use is observed. We feel that this change will be
sufficient to discourage "hackers", although it is obviously
insufficient to protect a node against a determined and malicious
attack.

    It should be noted that it is not our current intent to prohibit
occasional use of DDT for communication between sites via "DDT"
messages. Currently, there are two DDT commands, C and L, which set the
single-character message and multi-character message headers
respectively. We will continue this facility, either by always
permitting the use of these DDT commands, or by implementing some new
code outside DDT for this purpose.

            [This RFC was put into machine readable form for entry]
            [into the online RFC archives by Alex McKenzie with   ]
            [support from GTE, formerly BBN Corp.   10/99]