Secure operation of the domain name infrastructure is vital to the
global Internet community. Significant compromise of this infrastructure
could adversely effect national security and the global economy.

Over the years, several vulnerabilities to the domain name
infrastructure have been demonstrated. This summer, one particularly
dangerous vulnerability was demonstrated by Daniel Kaminsky. Although
exploitation of this vulnerability was not wide-spread, the Internet was
at risk until it was mitigated.

In order to protect the domain name infrastructure from vulnerabilities
like Kaminsky's, the Internet community must deploy DNSSEC as soon as
possible. While it is tempting to defer DNSSEC deployment until we have
refined and optimized the root zone signing procedure, this luxury is
not available to us. We must sign the root zones and deploy DNSSEC
before the next vulnerability leads to significant compromise.

Therefore, I support the proposal submitted by the Internet Corporation
for Assigned Names and Numbers (ICANN). In my opinion, this proposal
strikes an appropriate balance of responsibilities among the United
States Government, ICANN and VeriSign.

While I support the ICANN proposal and believe that it must be
implemented as quickly as possible, would like to add the following
comments:

ICANN should make clear that it is the custodian, and not the owner, of
the key-signing and zone-signing keys. While ICANN generates, uses and
protects those keys, it makes no claim to ownership. Therefore, it
cannot use those keys for any purpose other than that described in its
proposal to NTIA.

Furthermore, at some time in the future, the Internet community may
revisit the root zone signing procedure and determine that the ICANN
proposal no longer meets its needs. At that point, responsibilities and
key custodianship may need to be reassigned.
DISCLOSURE and DISCLAIMER: Ron Bonica is currently employed by Juniper Networks and currently serves as co-director of the IETF Operations and Management Area. The opinions stated in this memo are his, and do not necessarily represent those of his employer or the IETF.