Security for Domain Name System—Ready for Prime Time:

Chair: Olafur Gudmundsson, NAI

Panelists: David Conrad Executive Director Nominum/ISC
Edward Lewis, NAI
John Nguyen, DISA

A secured Domain Name System is becoming an operational reality with the latest release of the BIND software by the Internet Software Consortium. Strong interest in Europe, at the country-code and other top level delegations (including ".com" and ".mil"), and the root zones is shaping the way in which a secured DNS will operate now and into the future. The time is coming when each record in the system can be verified back to its source.

Besides being able to trust the name to address mapping, DNS will offer benefits to other protocols. By making public keys available through DNS, host to host and application to application exchanges can be secured. By accommodating certificates, PGP and X.509 data can be made available through the wide spread DNS. Through adding client (resolver) to server security, DNS can be reliably used to accommodate dynamic data, e.g., to reflect the movement of a computer through the network.

DNS is one of the core infrastructure technologies of the Internet. This panel will be of interest in learning how it can be secured and anyone that wants to make plans to take advantage of DNSSEC.