

# NIST Trustworthy Email Project

Scott Rose, NIST

[scottr@nist.gov](mailto:scottr@nist.gov)

ICANN Meeting Oct. 15<sup>th</sup>, 2014

Los Angeles CA

# First, A Bit of History

- 2011 USG DNSSEC Tiger Team has a 2<sup>nd</sup> goal: authenticated email
  - Deployment of Sender Policy Framework (SPF) and Domain Keying (DKIM) seen as first step
  - Authenticated email seen as vital for G2G and G2C communications
    - Right now, agencies explicitly state never to trust unsolicited email originating from them.
- DNSSEC seen as the enabling technology

# NIST HAD Project

- Enterprise level email security
  - SPF/DKIM/DMARC deployment
  - SMTP over TLS using DANE
- End-to-End email security using the DNS as a trust infrastructure
  - OpenPGP
  - S/MIME

# What HAD is Doing

- Monitoring for security artifacts in DNS
  - USG, banks, EDU
- Interactive test tools
  - SPF/DKIM/DMARC
  - OPENPGP
  - SMIMEA
- Guidance Documents
  - NIST Special Publications
- Protocol specifications

<https://www.had-pilot.com/>