



## DNSSEC Readiness Checklist

### Internet Service Providers (ISPs)

- Are you running Name Servers?
  - What version of BIND /NSD?
  - Is the BIND /NSD version NSEC3 aware?
    - BIND versions 9.6.0 and later support NSEC3.
    - NSD versions 3.1.0 and later support NSEC3 by default, NSD versions 3.0.0 and later support NSEC3 when turned on at compile time.
- Are you running recursive Name Servers, NSEC3 aware?
- For this, BIND versions 9.6.0 and later support NSEC3.
- Unbound versions 0.10 and later support NSEC3.
- Do all of your sites where Name Servers are hosted are DNSSEC NSEC3 aware?
- Have performed DNSSEC audit for your hardware?
  - Routers
  - Switches
  - Firewalls
  - Load balancers
    - Common issues to check for:
    - Parsing DNS traffic and not understanding NSEC3 packets
    - Dropping packets > 512 bytes
    - Not allowing TCP traffic
- Is the customer premise equipment DNSSEC NSEC3 aware?
  - Ideally this means simply passing packets through.
  - Please review IETF draft with guidelines: <http://tools.ietf.org/html/draft-bellis-dnsexext-dnsproxy-00>