

# DNS COMPLIANCE

Fred Baker  
Internet Systems Consortium

# Background - 2014

ISC was in the process of adding DNS COOKIE (RFC 7873) to BIND and we wanted to see how many servers would mishandle DNS COOKIE options and in which ways as they would be sent with every query unlike other EDNS options that are only occasionally sent.

If we were going to measure how many servers would mishandle DNS COOKIE options we may as well measure how servers mishandle all EDNS extension mechanisms and track that over time.

<https://ednscmp.isc.org/>

Test your own servers

<https://ednscmp.isc.org/ednscmp>

draft-ietf-dnsop-no-response-issue

# Testing Method

- A series of queries for the SOA/DNSKEY RR-set at the zone's apex which tested specific aspects of EDNS behaviour.
- The responses were then examined to see if they matched the expected behaviour of a server that implements EDNS correctly.

# Type Testing

<https://ednscomp.isc.org/compliance/tld-typereport.txt>

- . @2001:7fd::1 (k.root-servers.net.): all ok
- . @199.7.83.42 (l.root-servers.net.): URI=notimp
- . @2001:500:9f::42 (l.root-servers.net.): all ok
- . @202.12.27.33 (m.root-servers.net.): all ok
- . @2001:dc3::35 (m.root-servers.net.): all ok

# Other DNS testing.

<https://ednscomp.isc.org/compliance/tld-fullreport.txt>

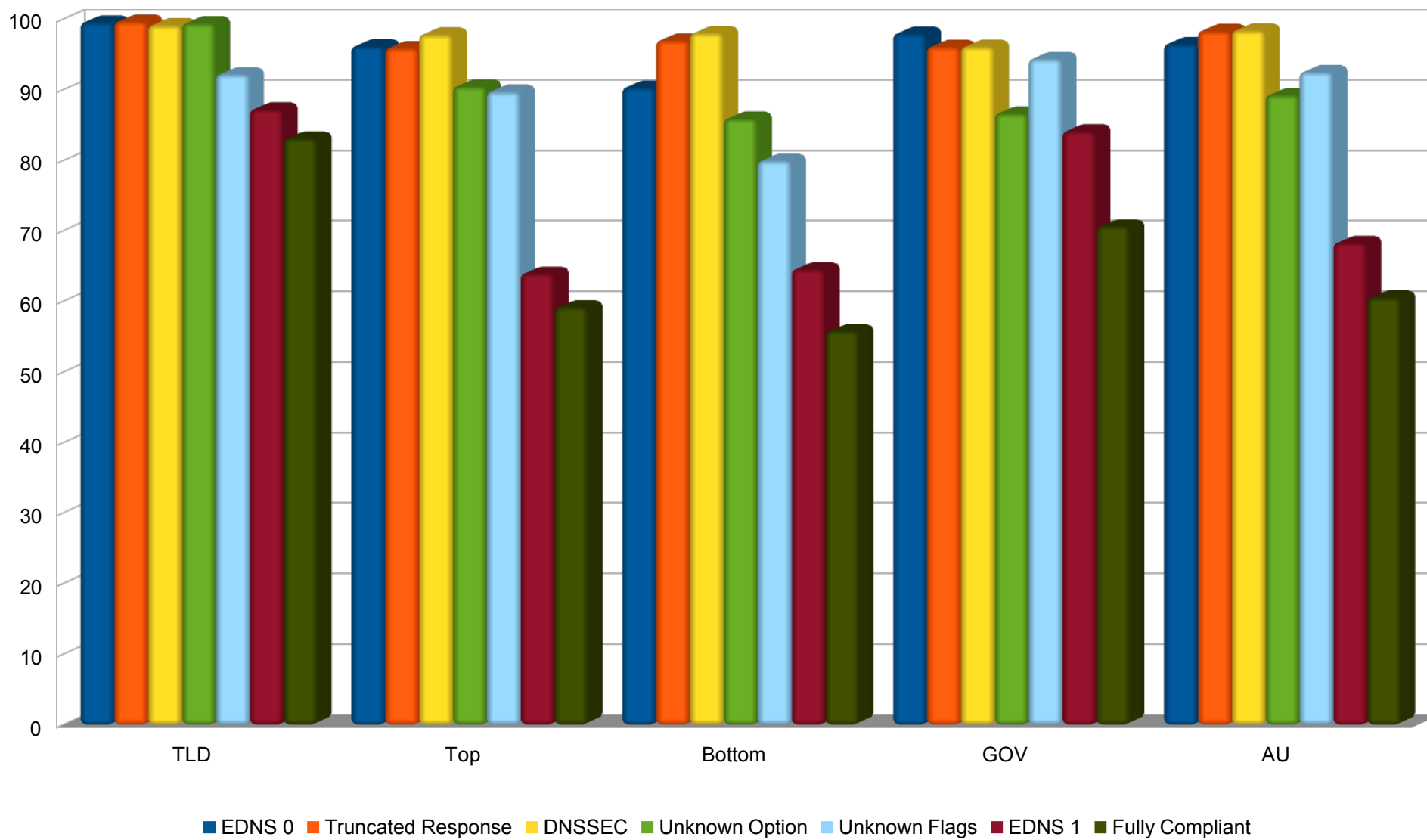
. @2001:503:ba3e::2:30 (a.root-servers.net.): dns=ok aa=ok ad=ok  
cd=ok ra=ok rd=ok tc=ok zflag=ok opcode=ok opcodeflg=reset  
type666=ok tcp=ok edns=ok edns1=ok edns@512=ok ednsopt=ok  
edns1opt=ok do=ok edns1do=ok ednsflags=ok optlist=ok  
ednsnsid=ok ednscookie=ok ednsexpire=ok ednssubnet=ok  
edns1nsid=ok edns1cookie=ok edns1expire=ok edns1subnet=ok  
signed=ok,yes ednstcp=ok

. @192.228.79.201 (b.root-servers.net.): dns=ok aa=ok ad=ok  
cd=ok ra=ok rd=ok tc=ok zflag=ok opcode=ok opcodeflg=rd,cd  
type666=ok tcp=ok edns=ok edns1=ok edns@512=ok ednsopt=ok  
edns1opt=ok do=ok edns1do=ok ednsflags=ok optlist=ok,nsid  
ednsnsid=ok,nsid ednscookie=ok ednsexpire=ok ednssubnet=ok  
edns1nsid=ok edns1cookie=ok edns1expire=ok edns1subnet=ok  
signed=ok,yes ednstcp=ok

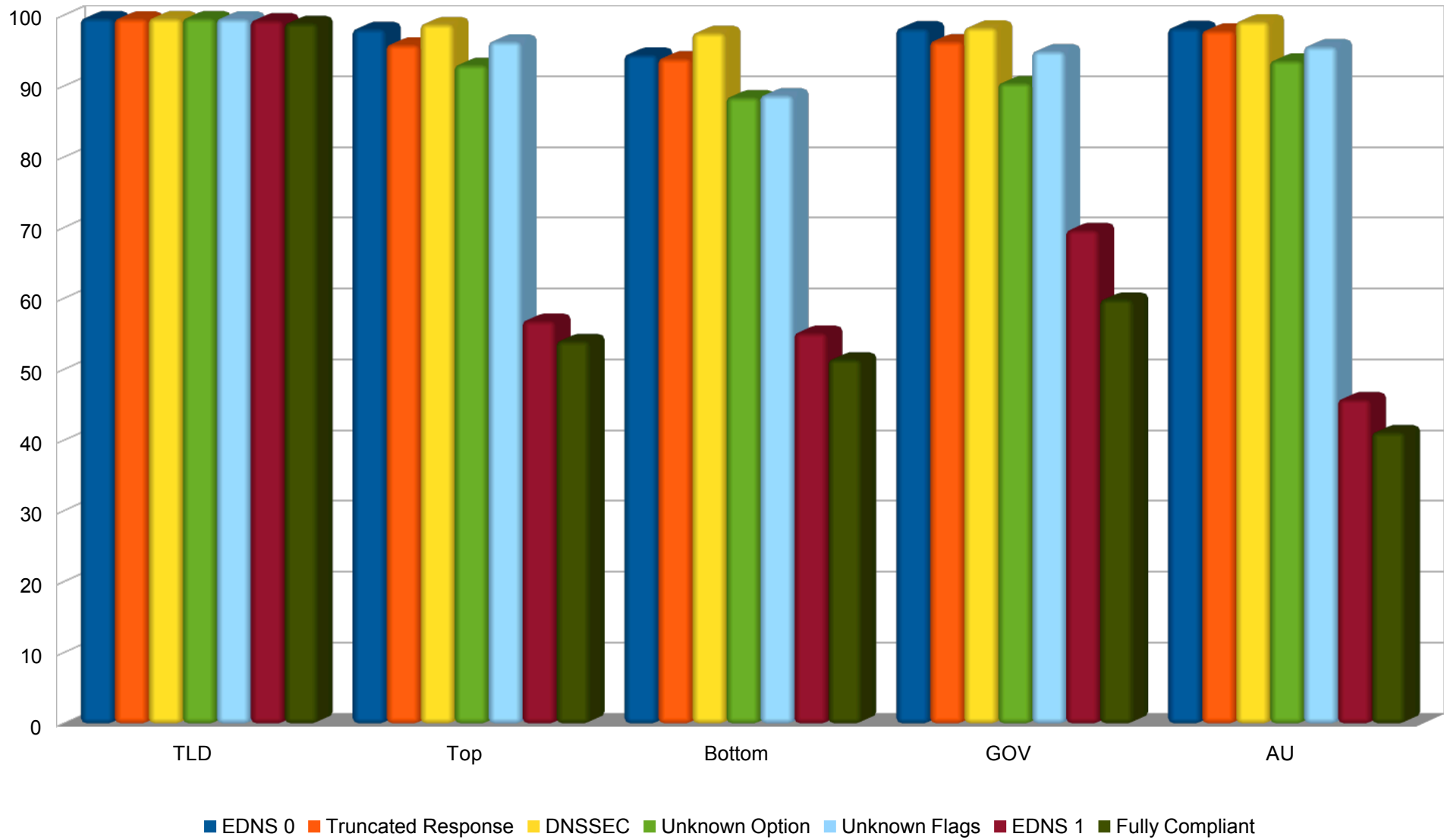
# Aims of talk

- To show the current state of EDNS compliance
- To show the impact of what will happen when different EDNS extension mechanism are used without taking proactive steps to fix the current issues

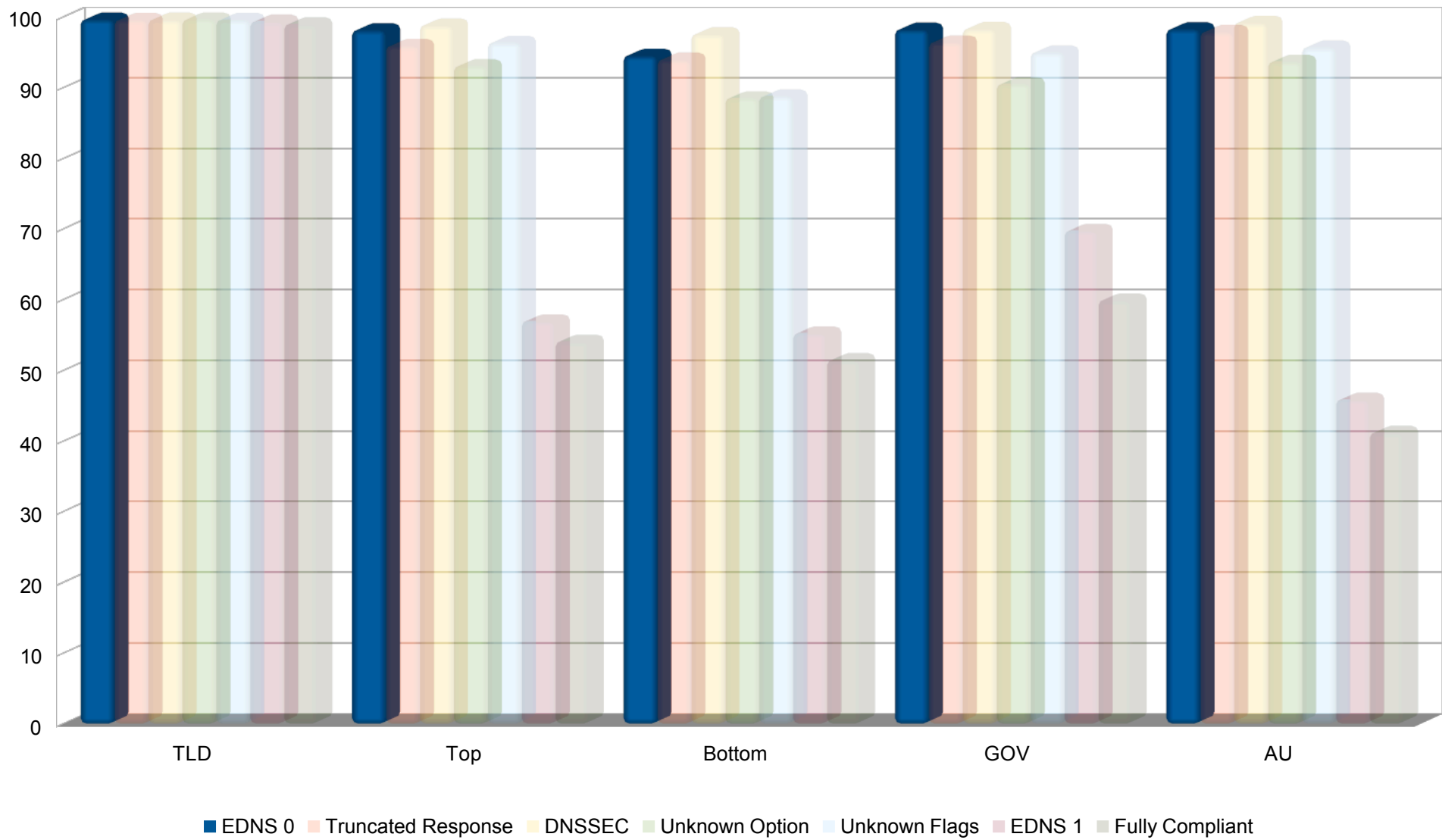
EDNS Compliance by Function of EDNS Aware Servers - 12 Sep 2014



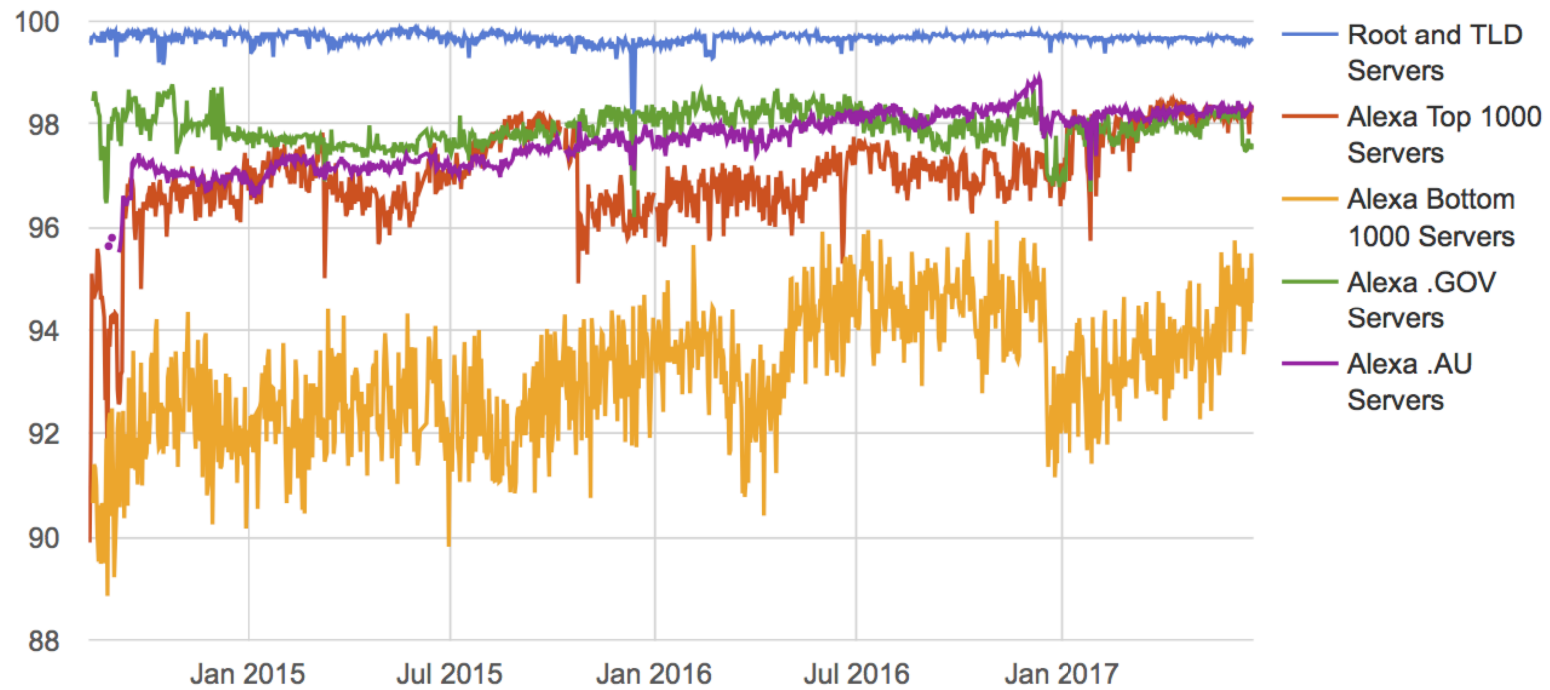
EDNS Compliance by Function of EDNS Aware Servers - 31 May 2017



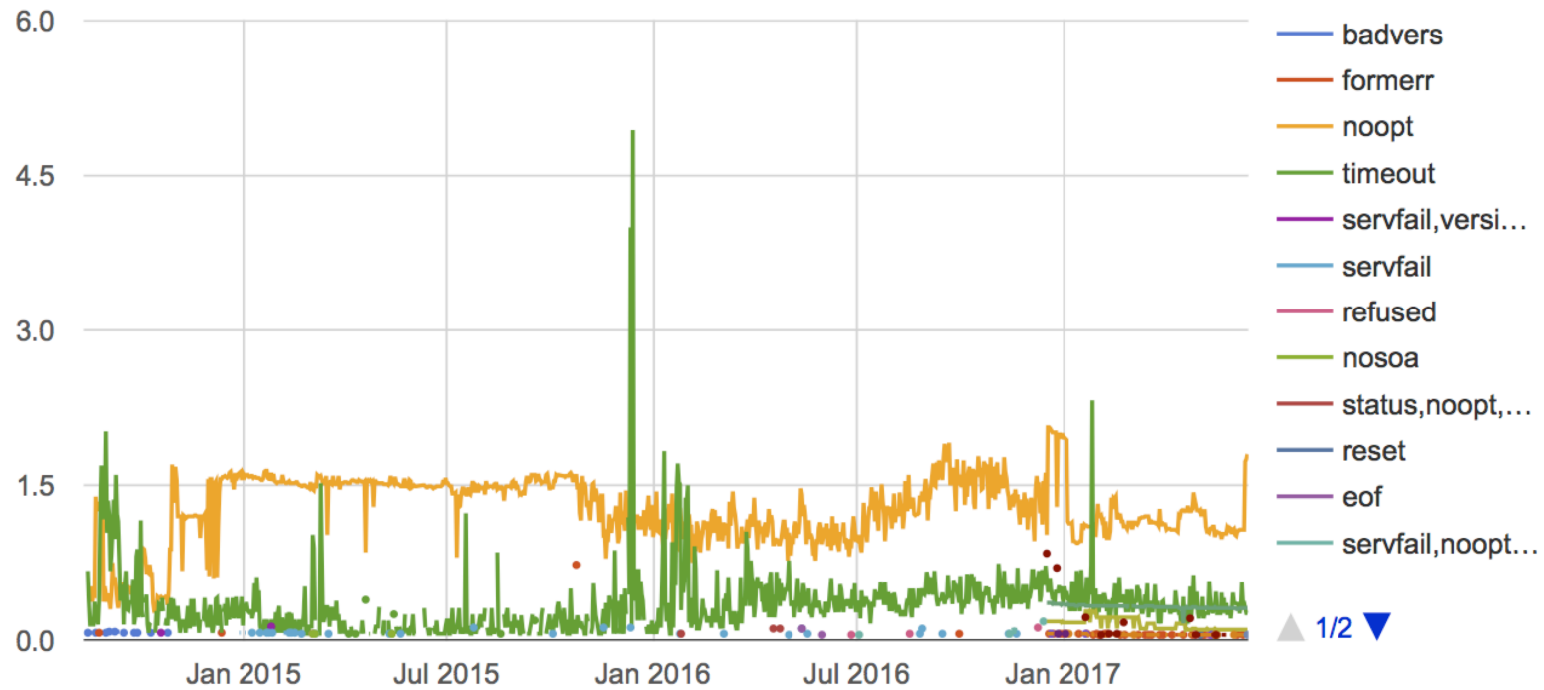
EDNS Compliance by Function of EDNS Aware Servers - 31 May 2017



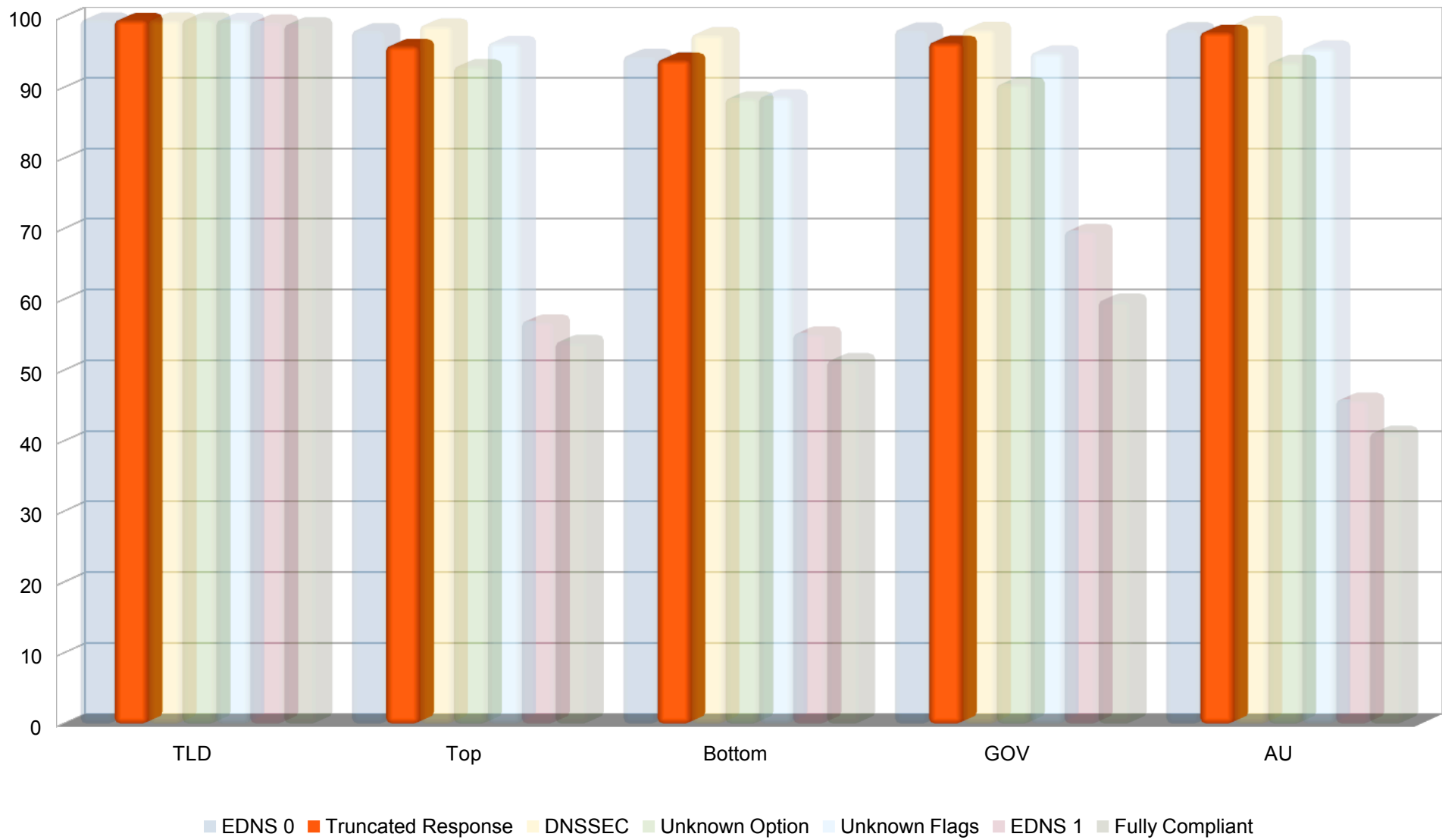
Percentage of EDNS aware servers that passed plain EDNS(0) check



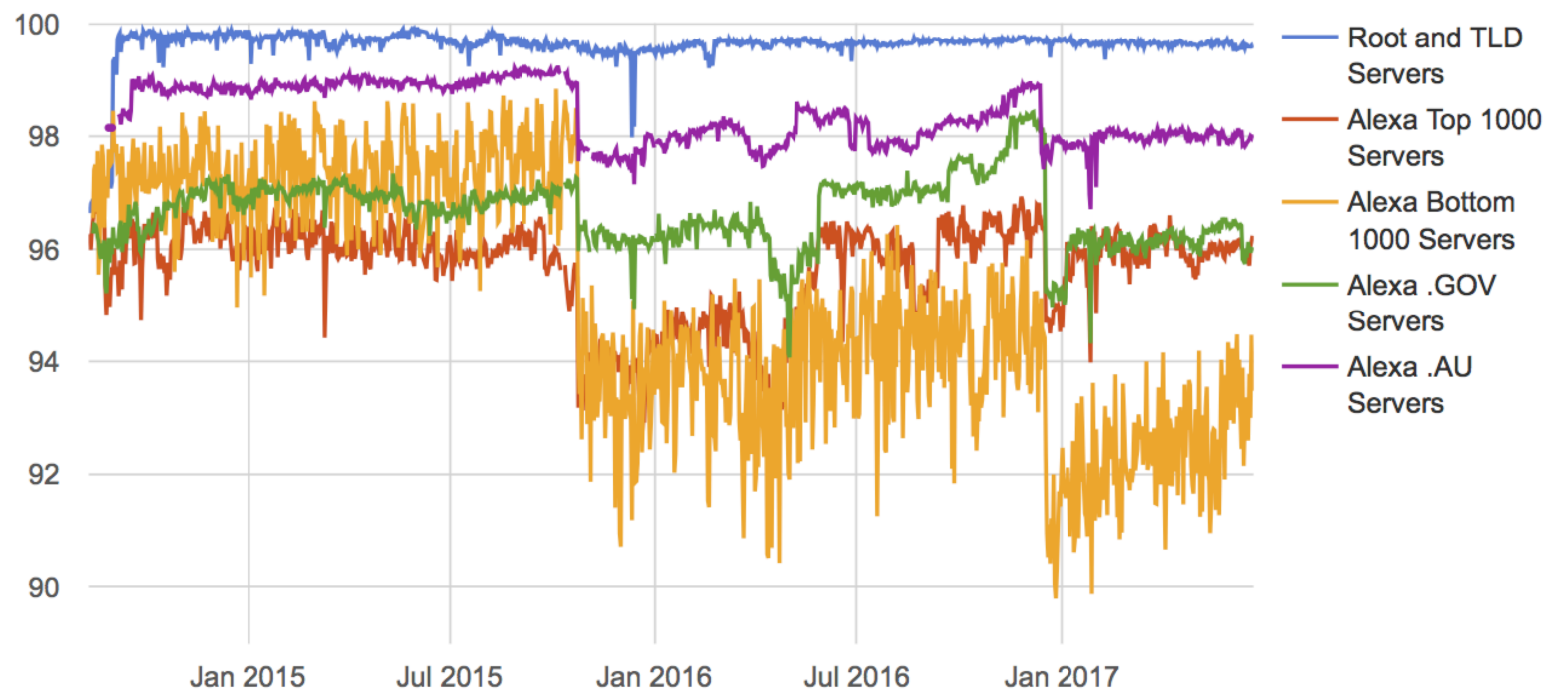
Alexa .GOV Servers EDNS(0) Failure Reasons



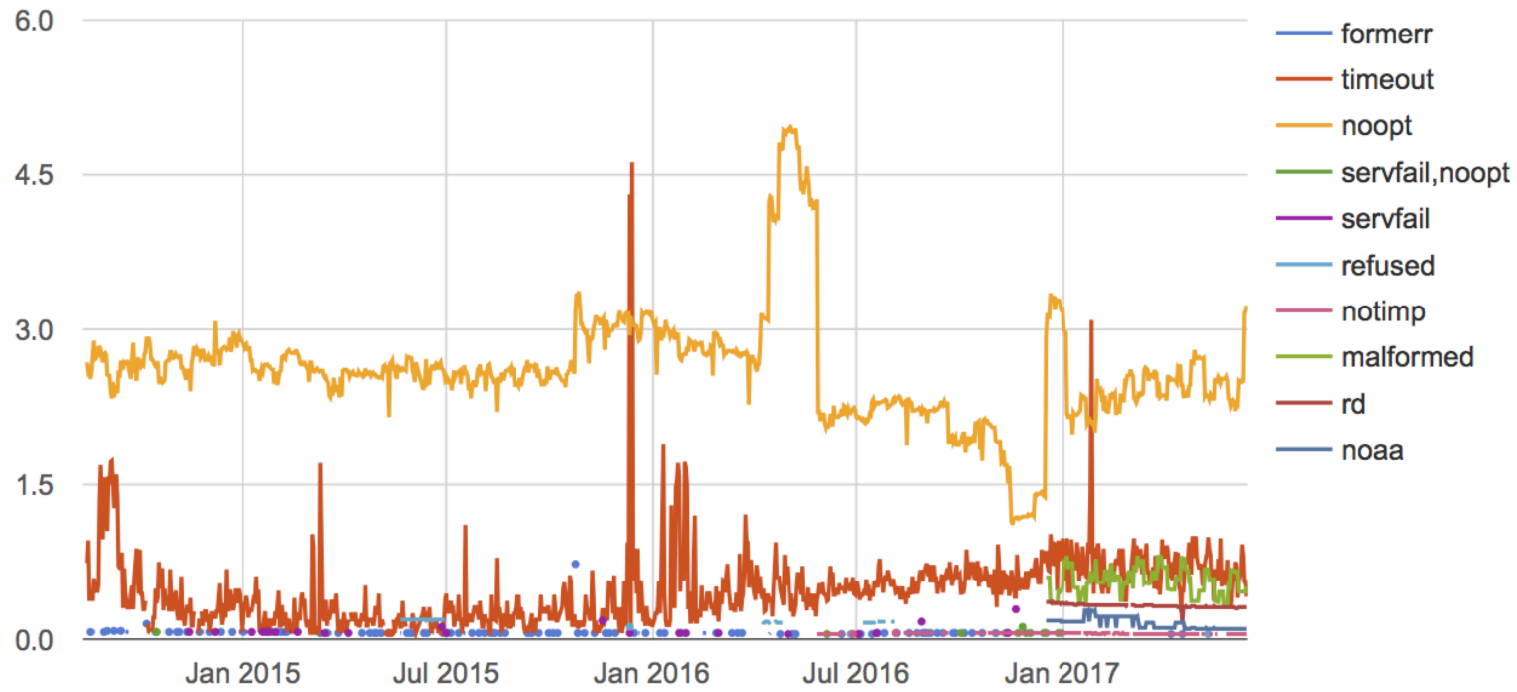
EDNS Compliance by Function of EDNS Aware Servers - 31 May 2017



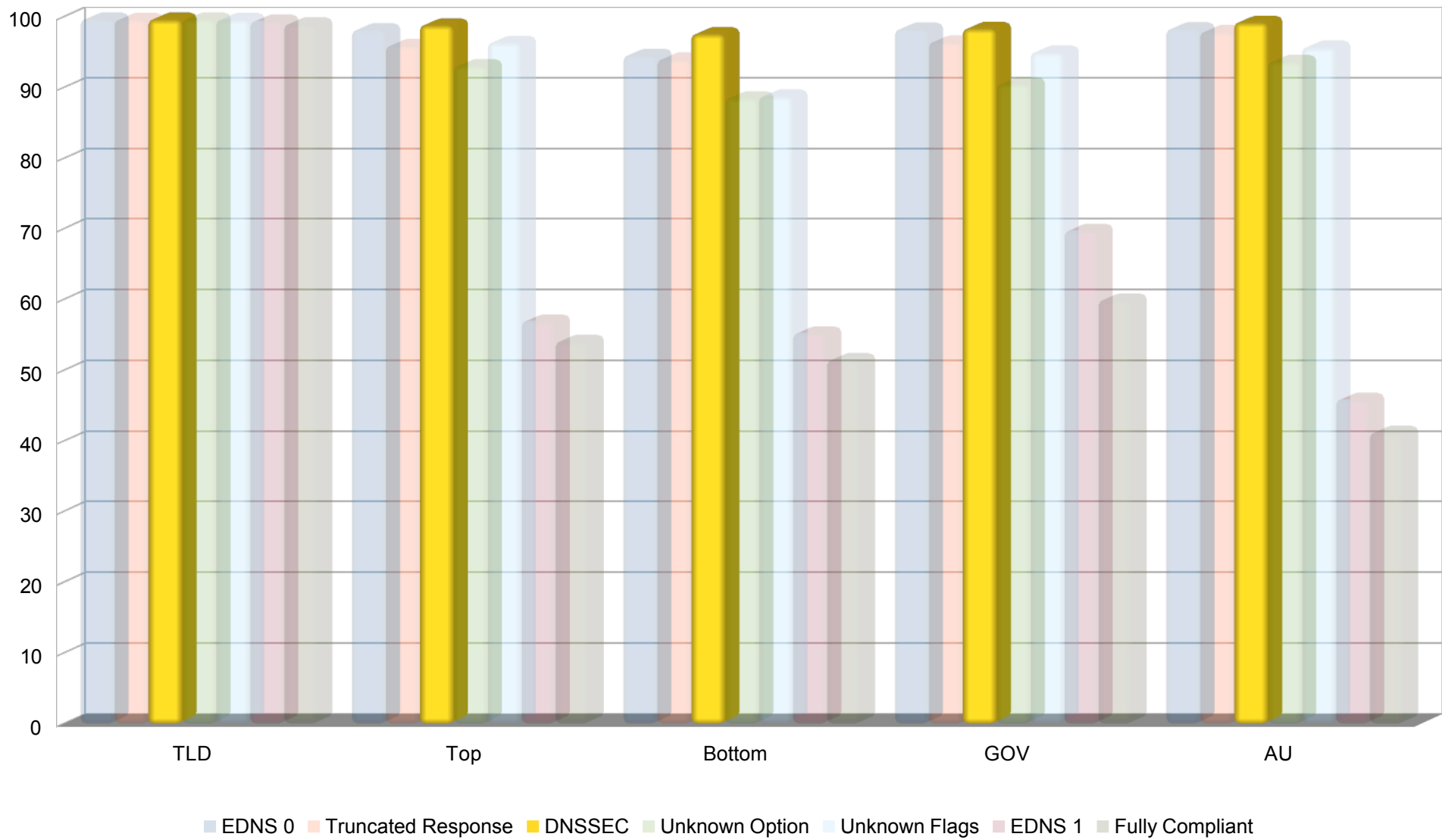
**Percentage of EDNS aware servers that returned OPT record in truncated EDNS(0) response**



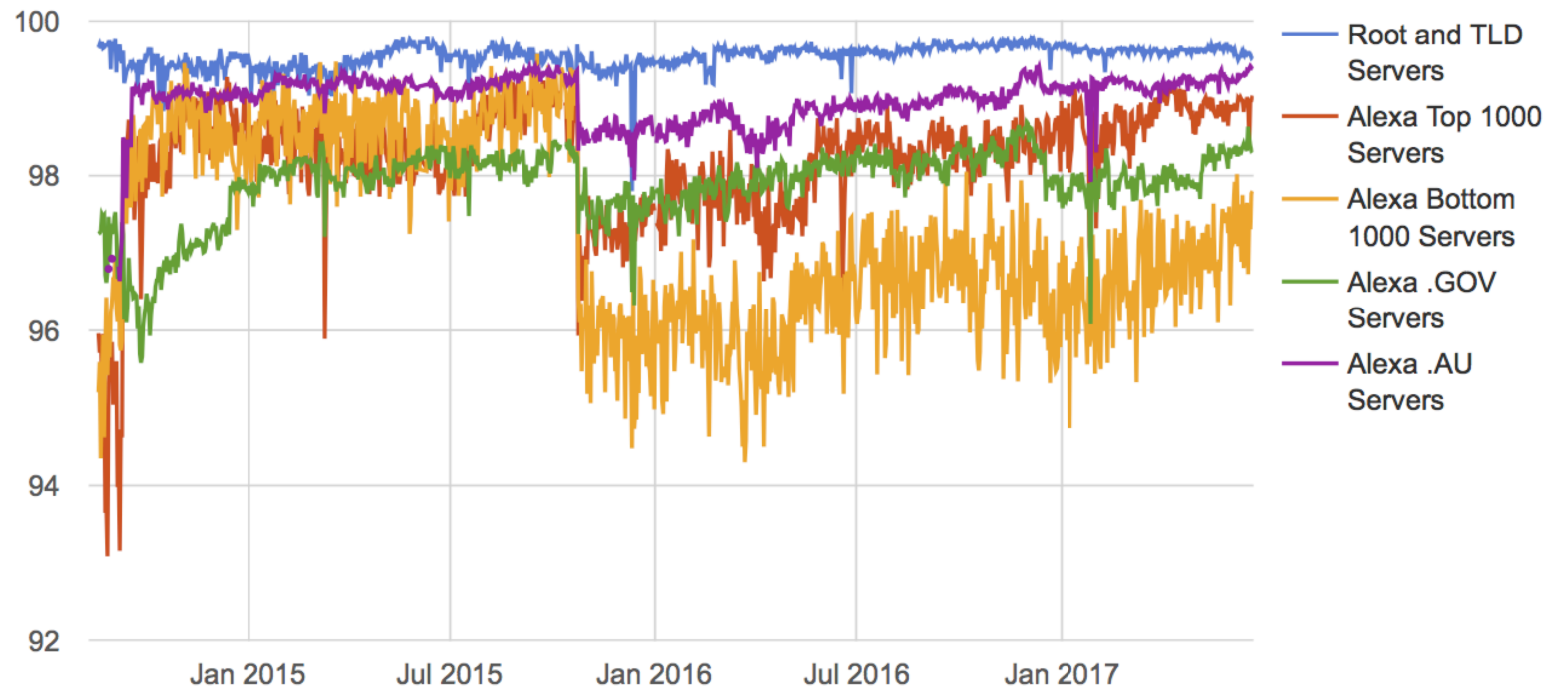
Alexa .GOV Servers EDNS(0) Truncated Response Failure Reasons



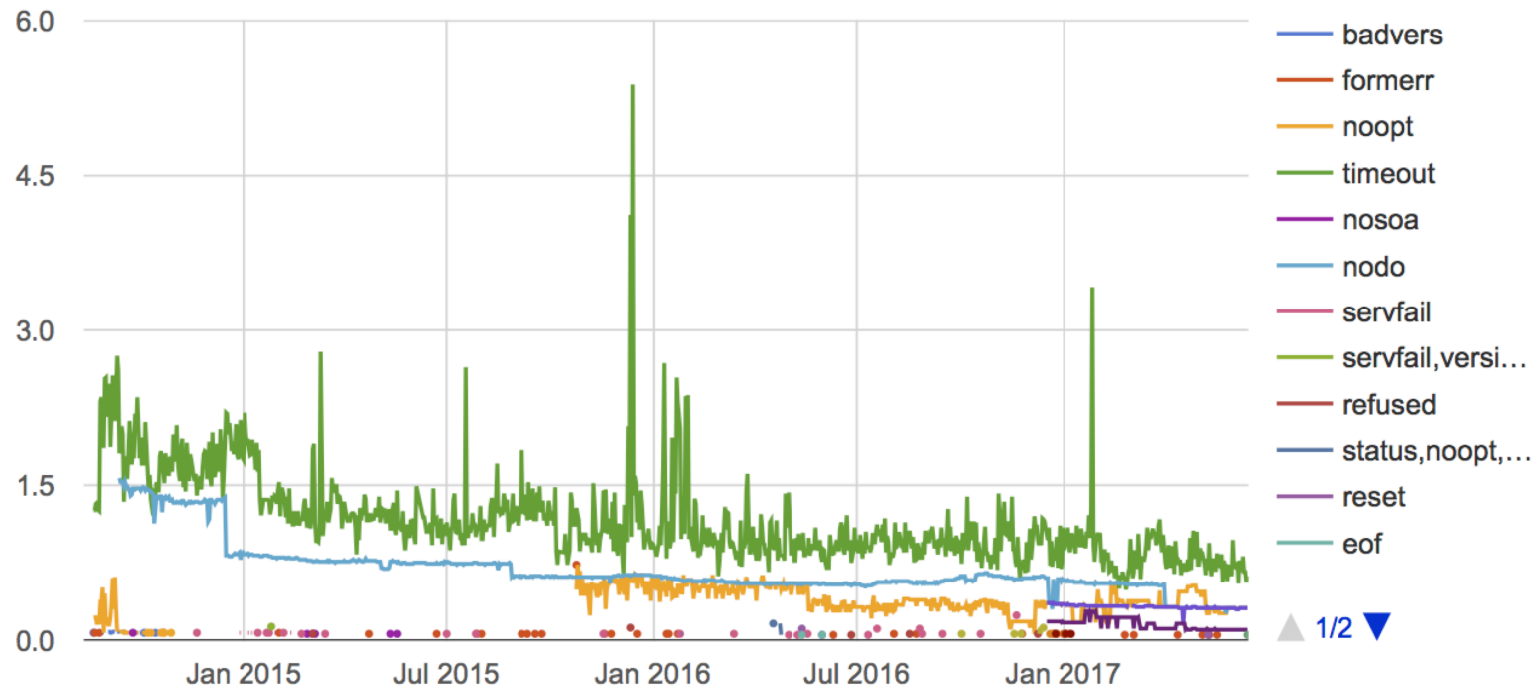
EDNS Compliance by Function of EDNS Aware Servers - 31 May 2017



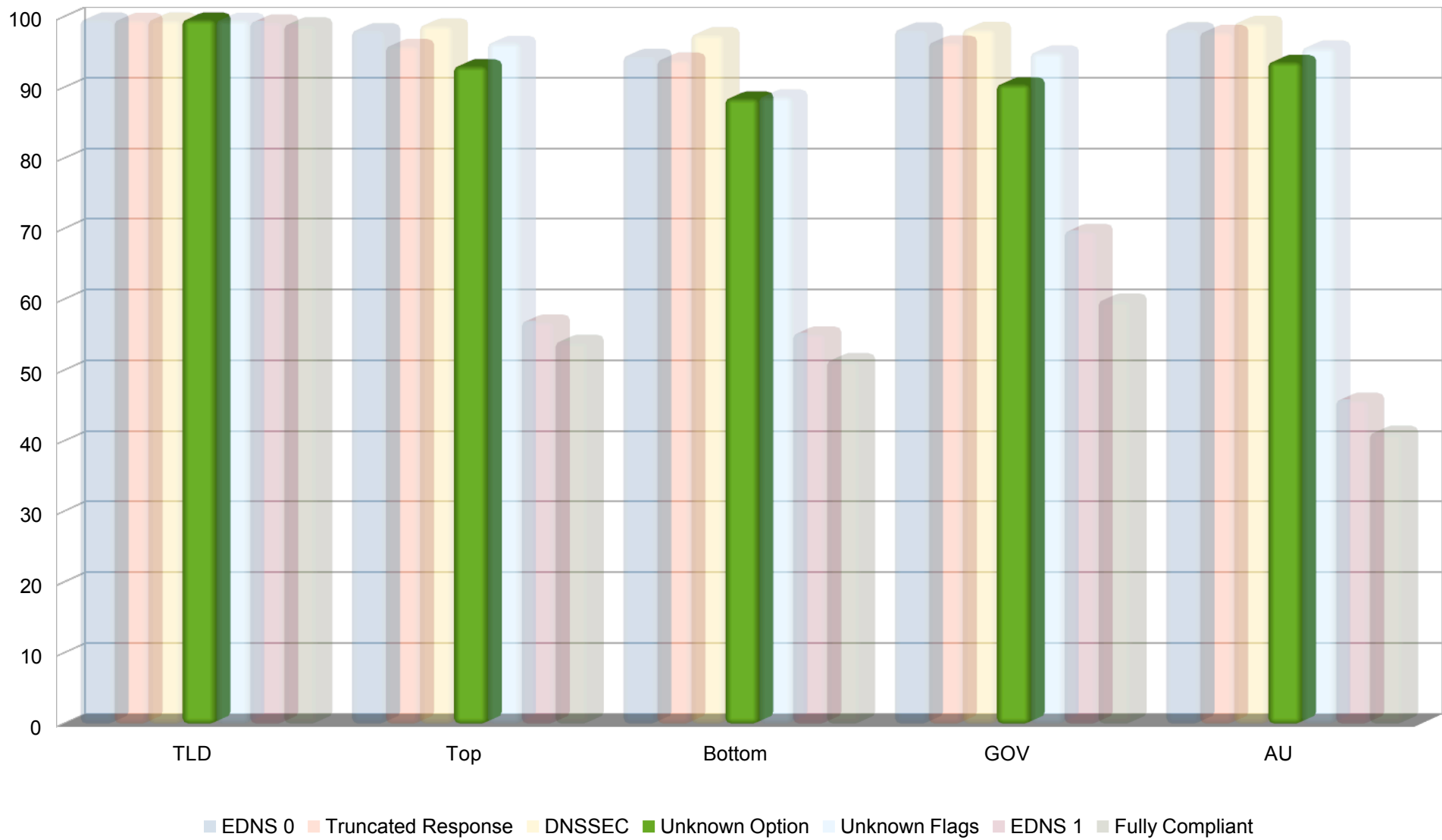
Percentage of EDNS aware servers that passed EDNS(0) + DO=1 check



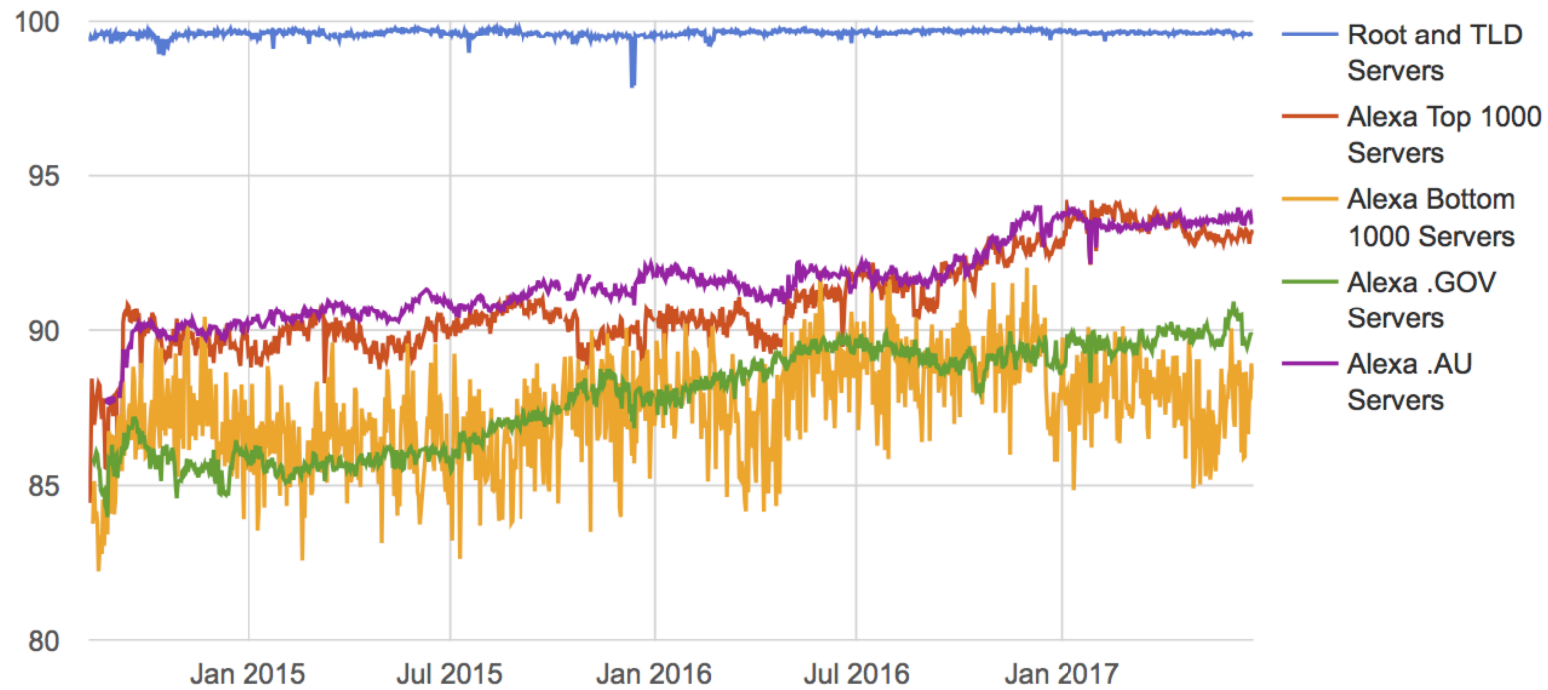
Alexa .GOV Servers EDNS(0) DO=1 Failure Reasons



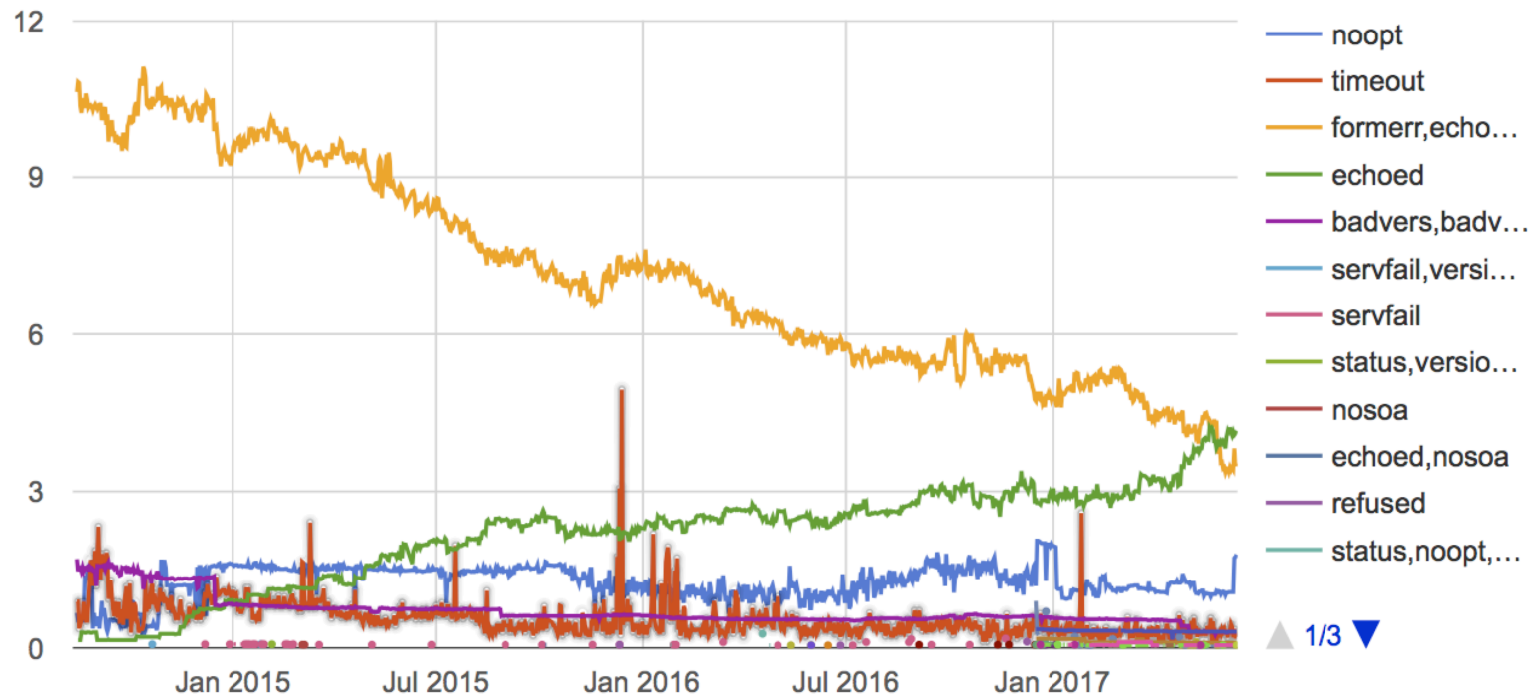
EDNS Compliance by Function of EDNS Aware Servers - 31 May 2017



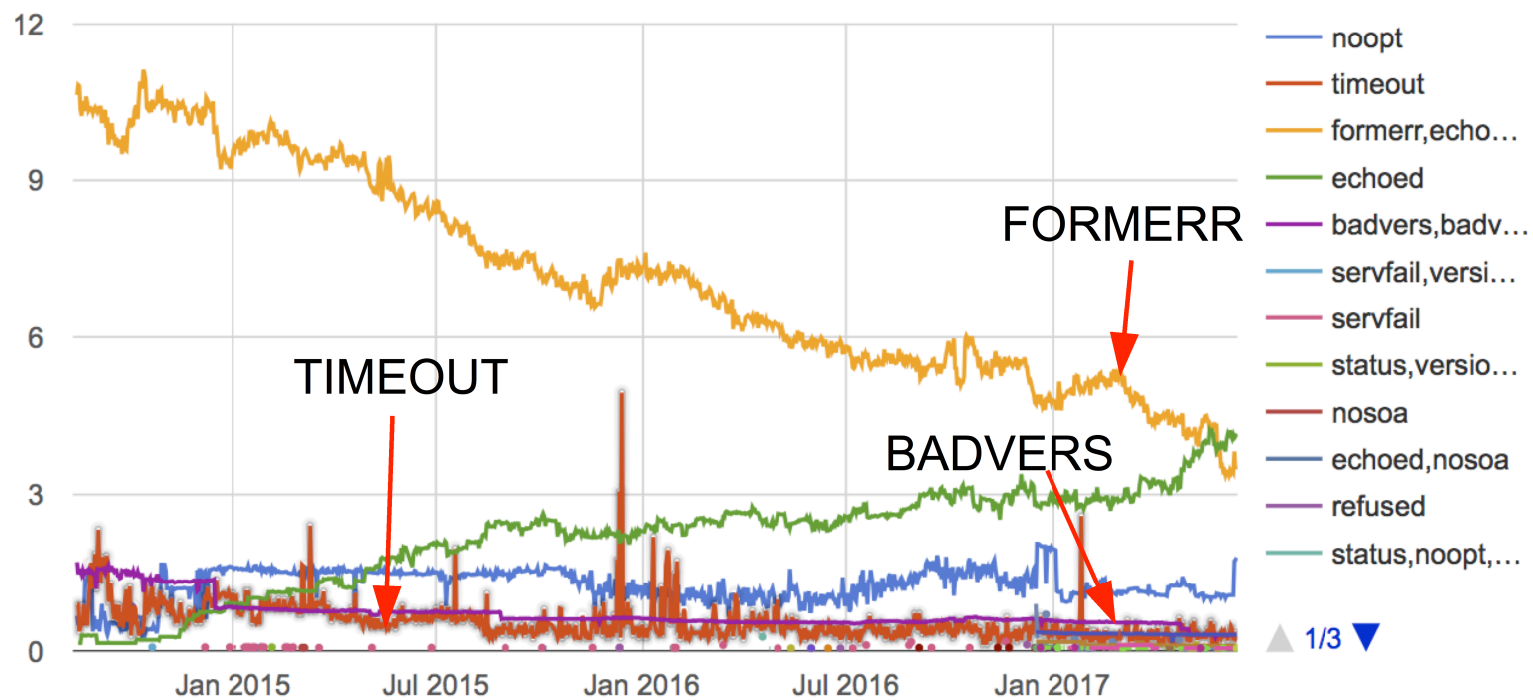
Percentage of EDNS aware servers that handled unknown EDNS(0) options correctly



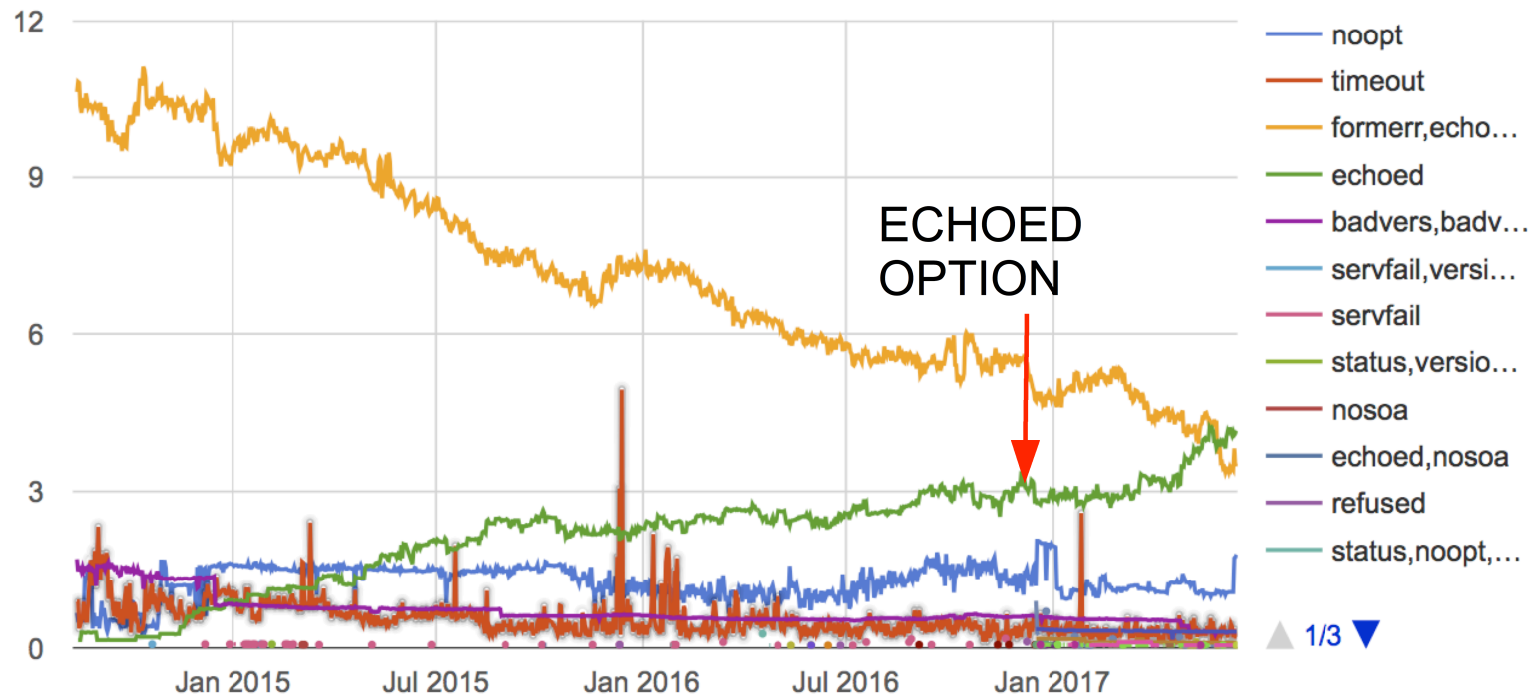
### Alexa .GOV Servers EDNS(0) Unknown Option Failure Reasons



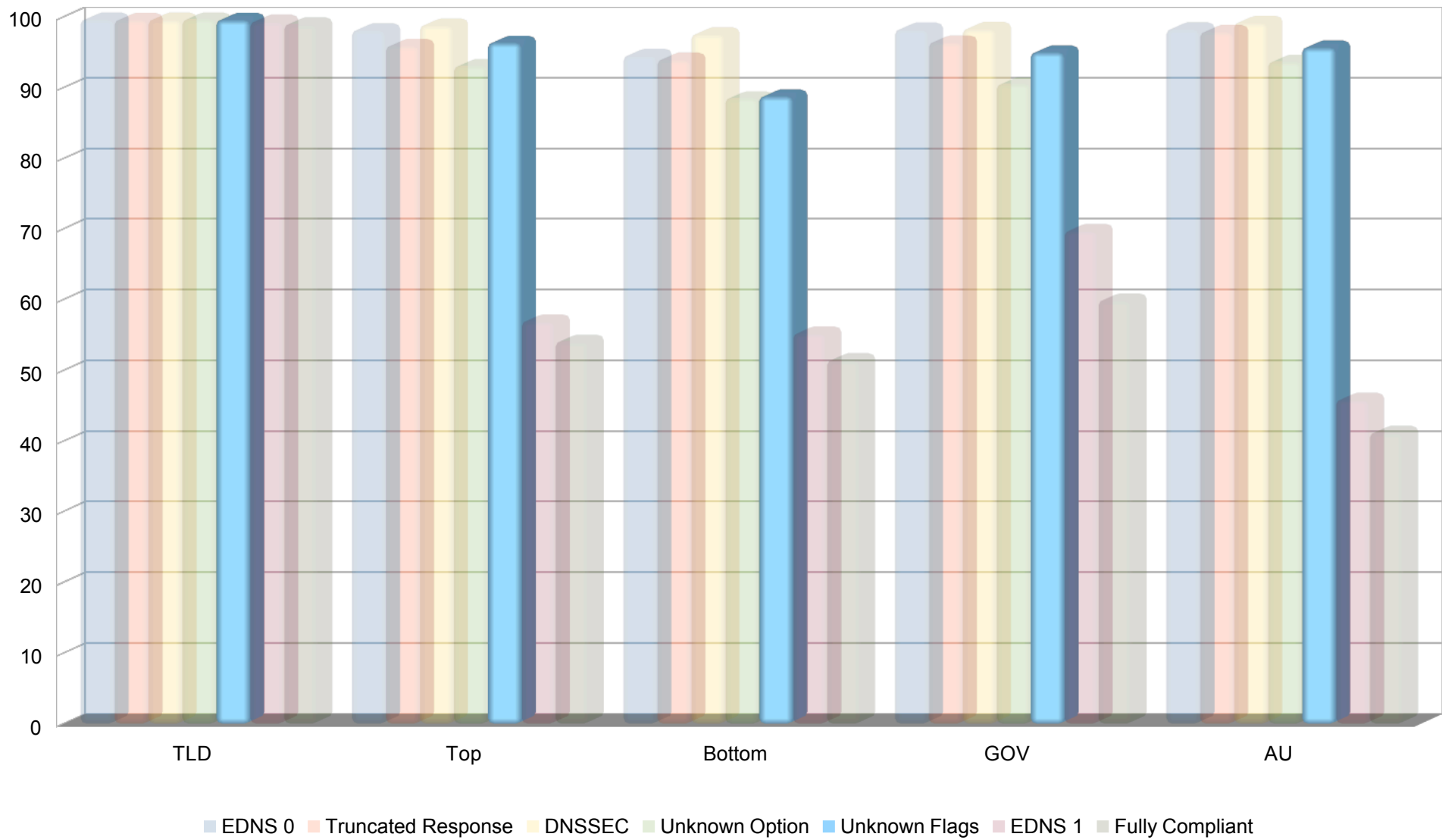
Alexa .GOV Servers EDNS(0) Unknown Option Failure Reasons



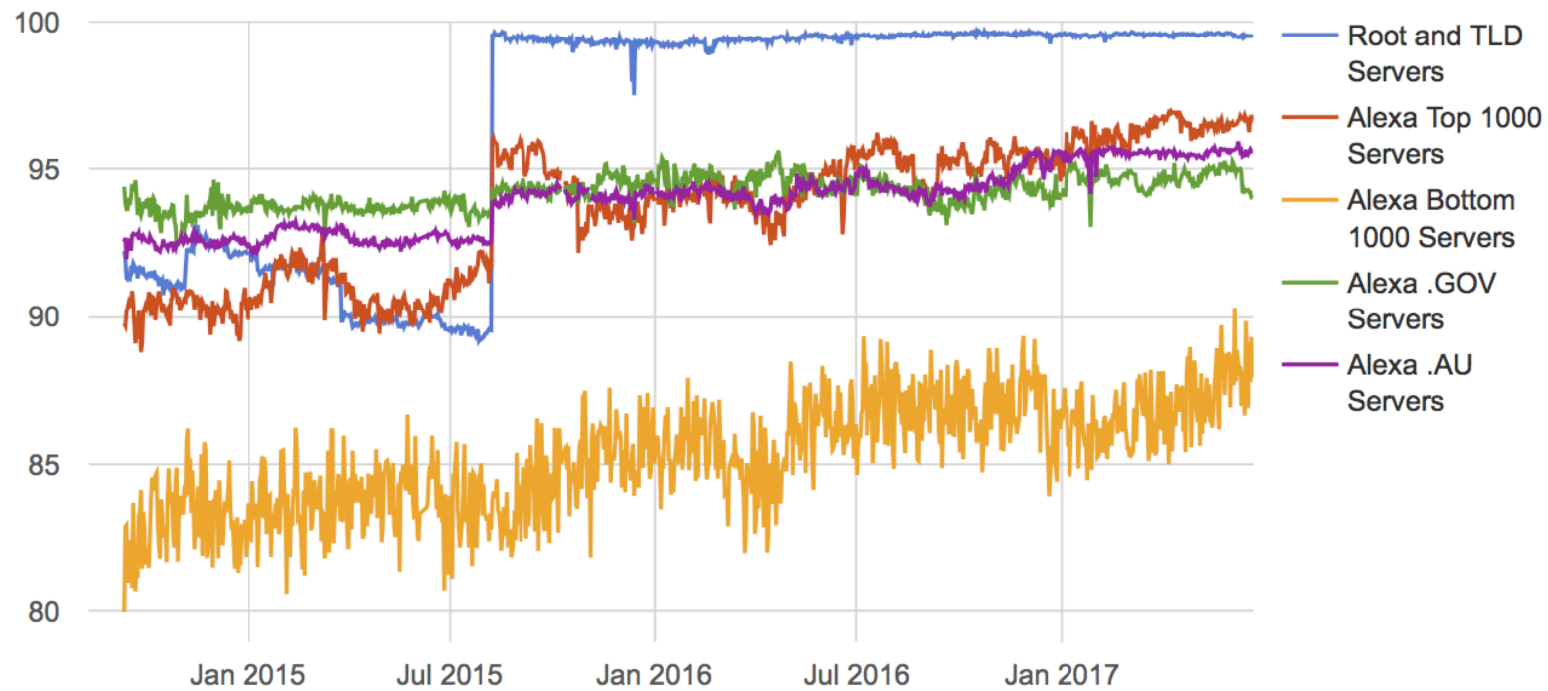
### Alexa .GOV Servers EDNS(0) Unknown Option Failure Reasons



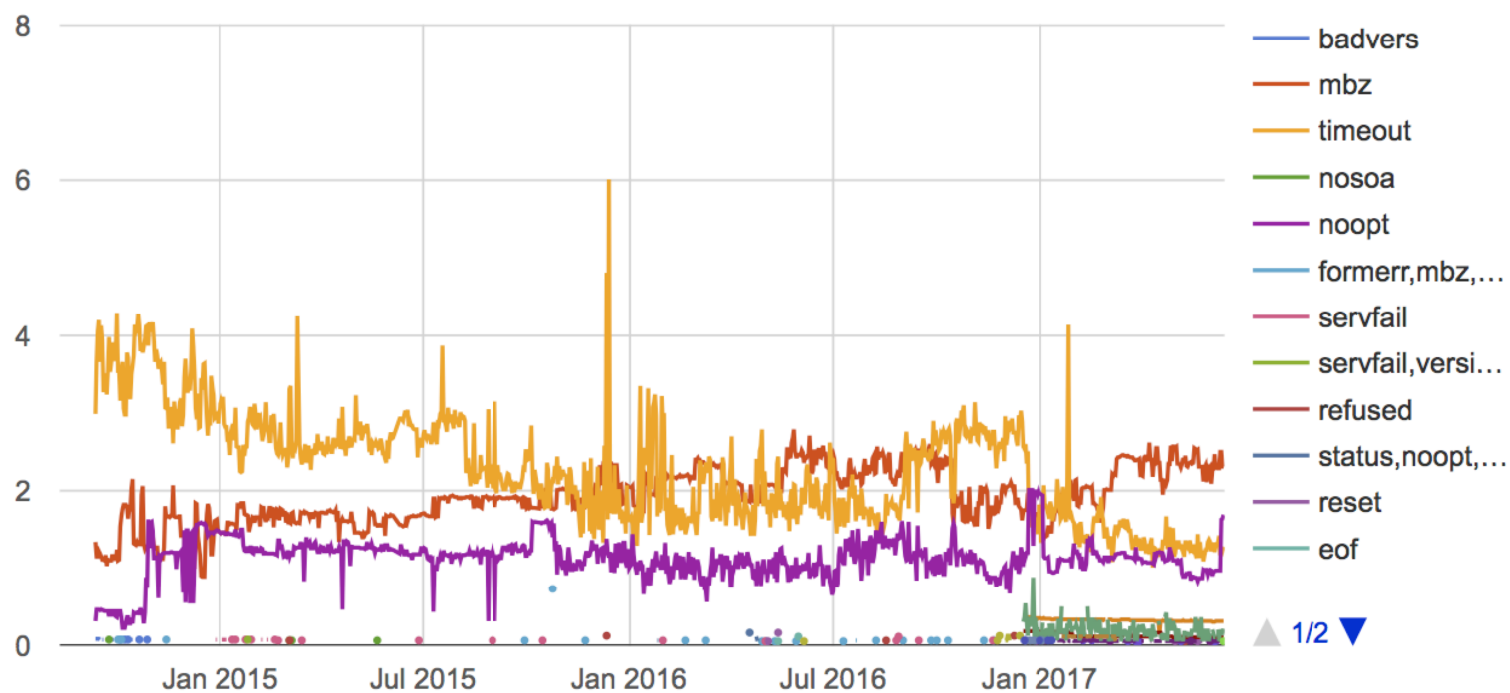
EDNS Compliance by Function of EDNS Aware Servers - 31 May 2017



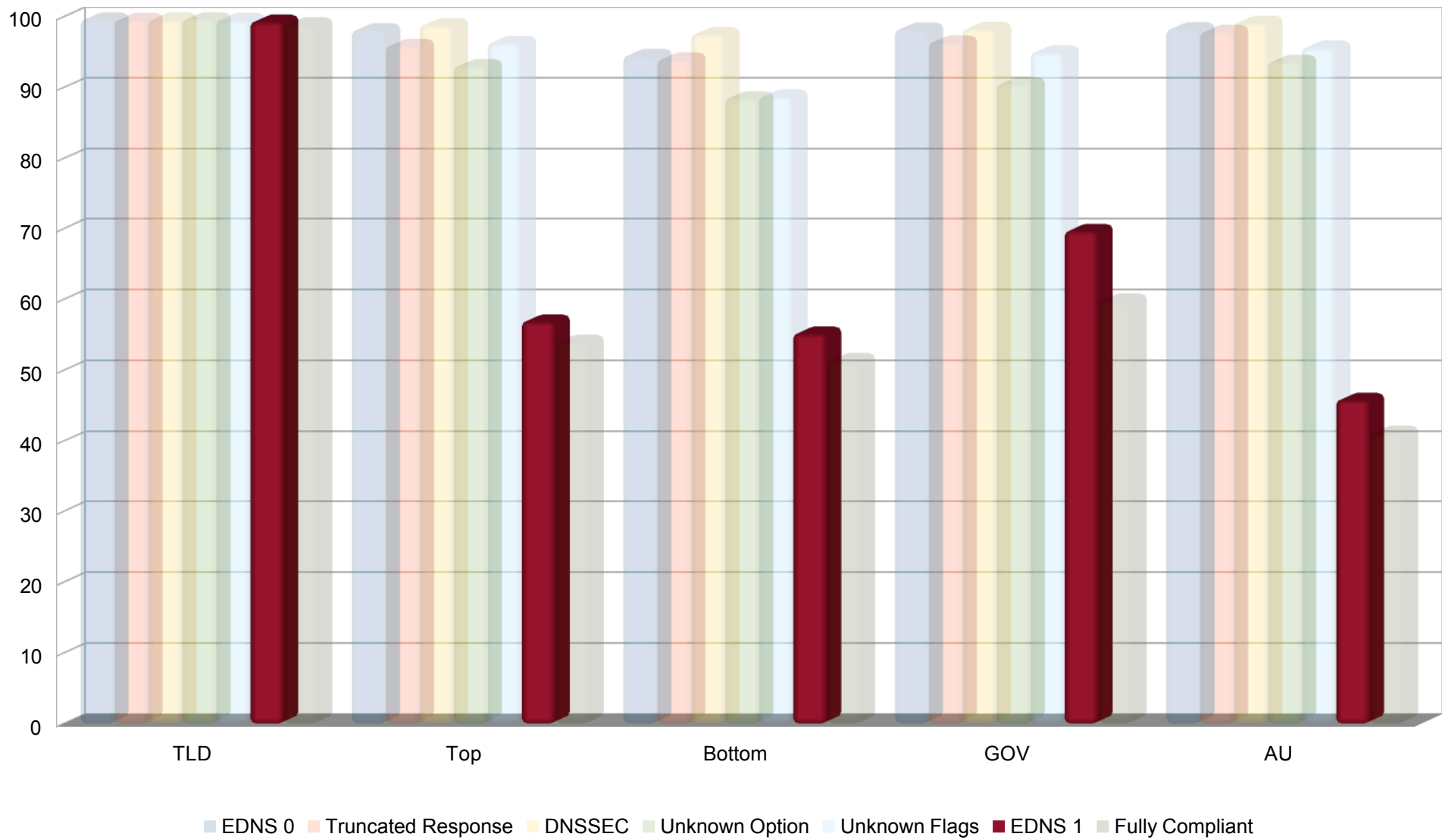
Percentage of EDNS aware servers that handled unknown EDNS(0) flags correctly



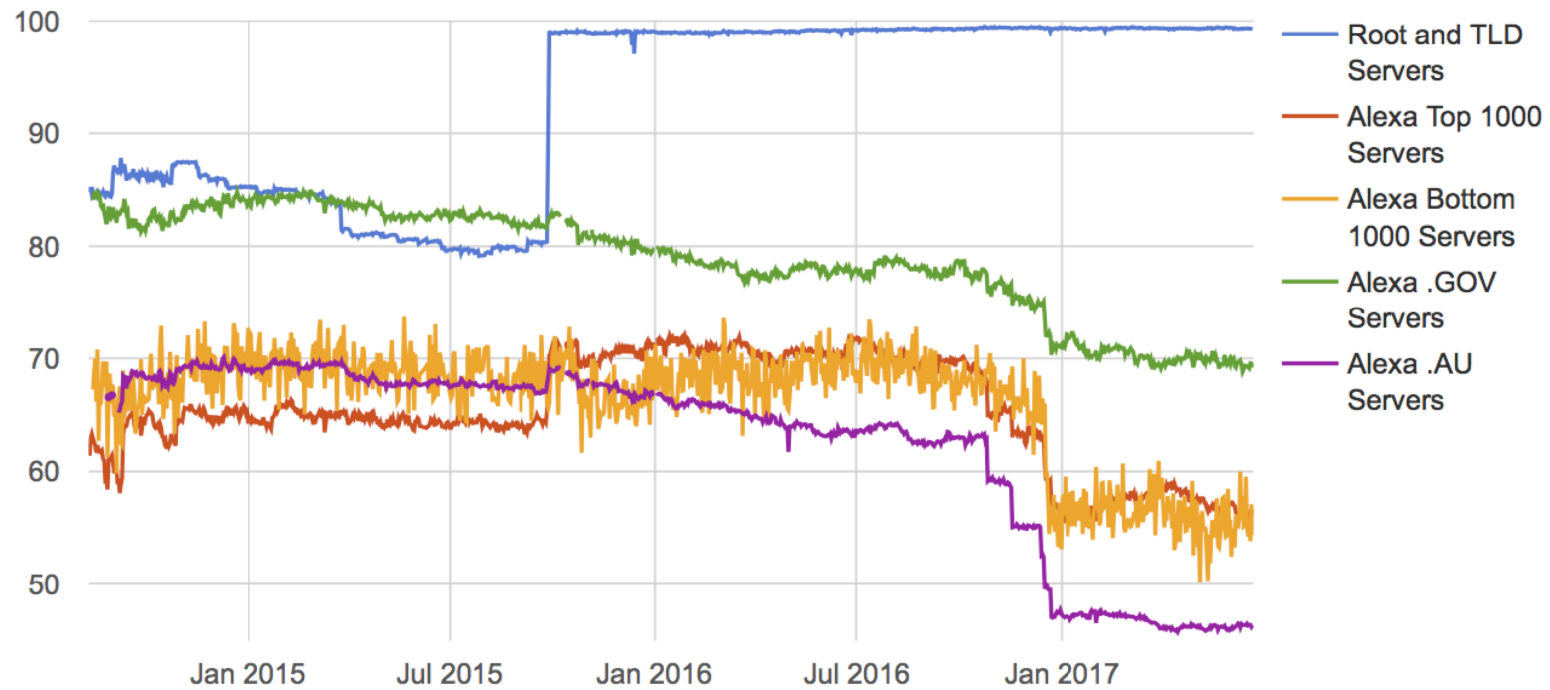
### Alexa .GOV Servers EDNS(0) Unknown Flags Failure Reasons



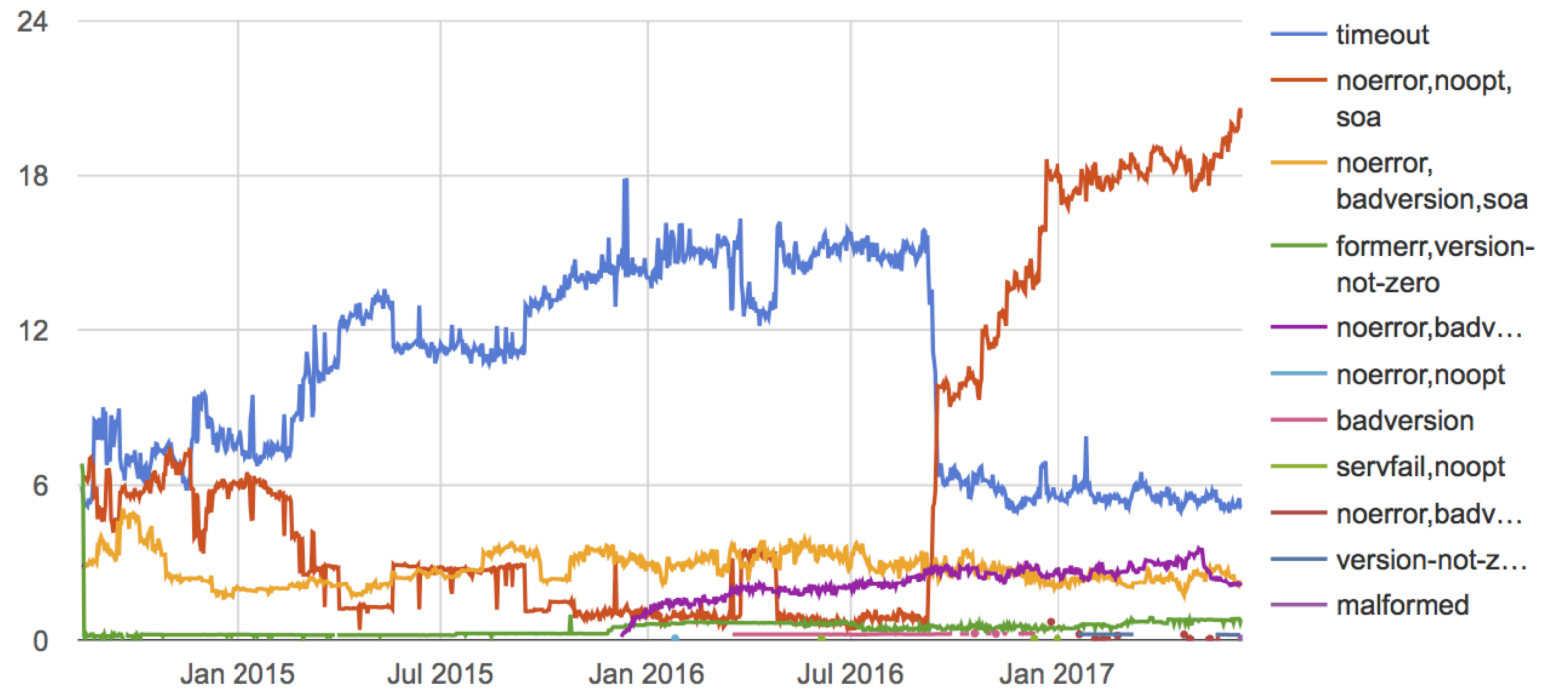
EDNS Compliance by Function of EDNS Aware Servers - 31 May 2017



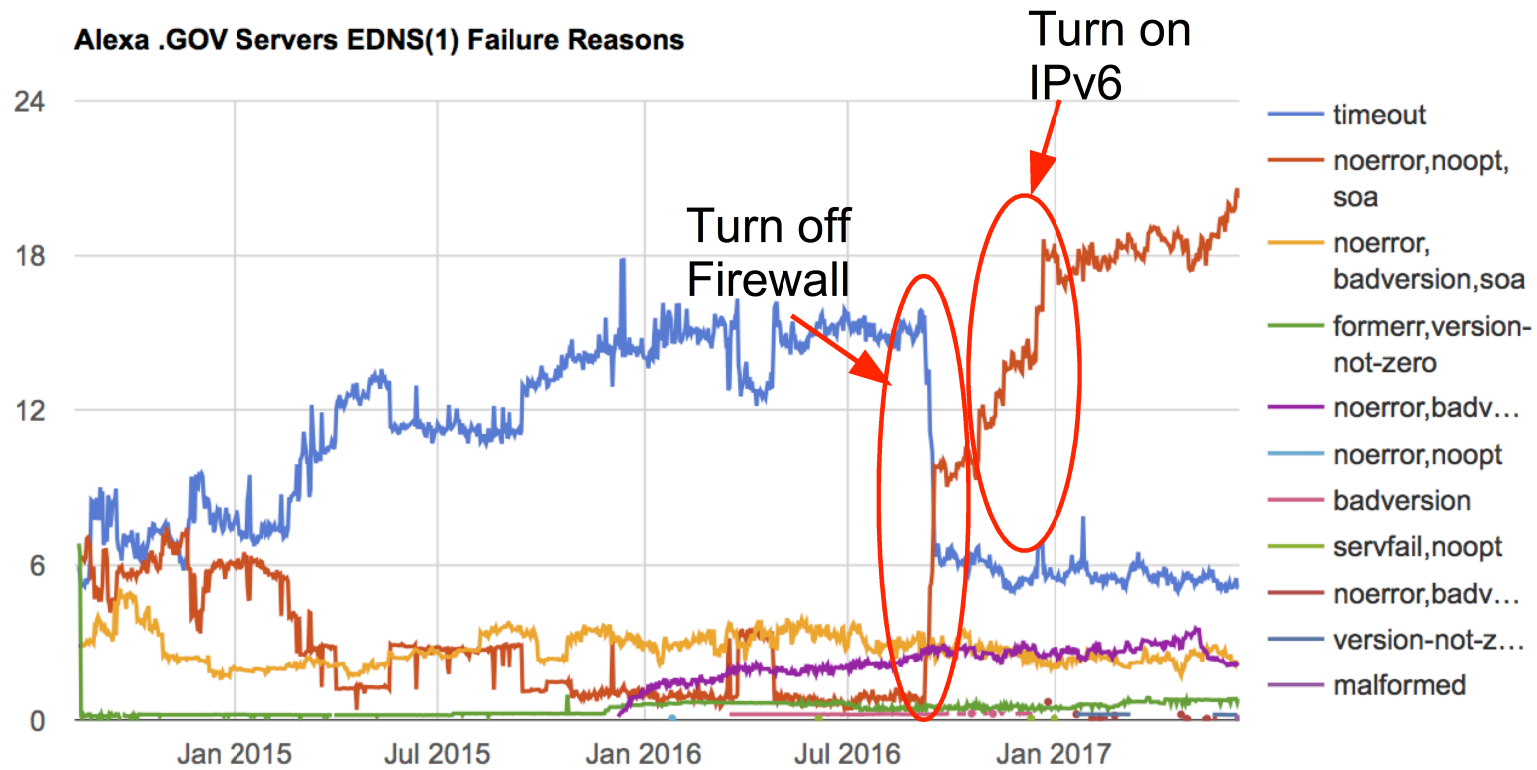
Percentage of EDNS aware servers that passed plain EDNS(1) check



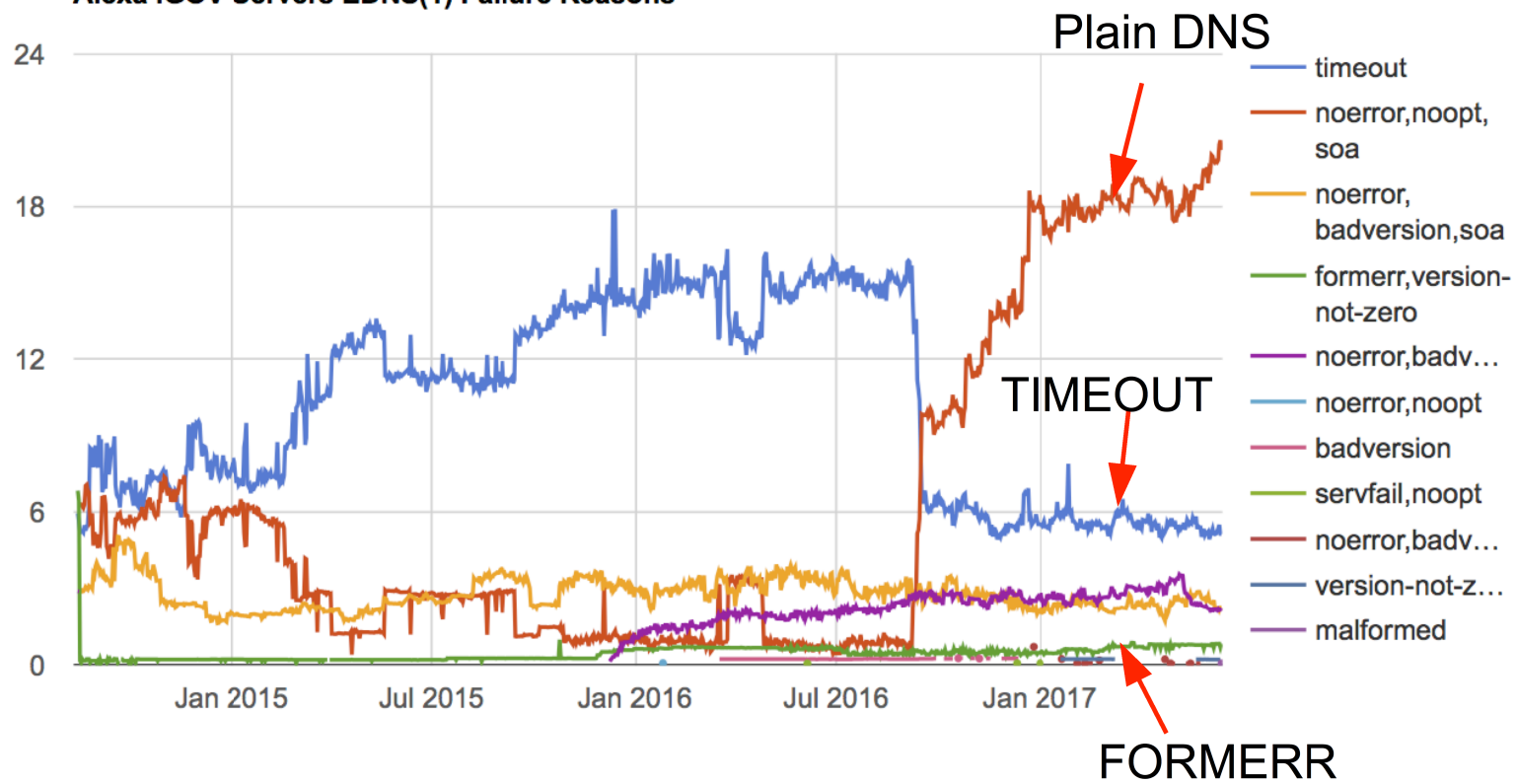
Alexa .GOV Servers EDNS(1) Failure Reasons



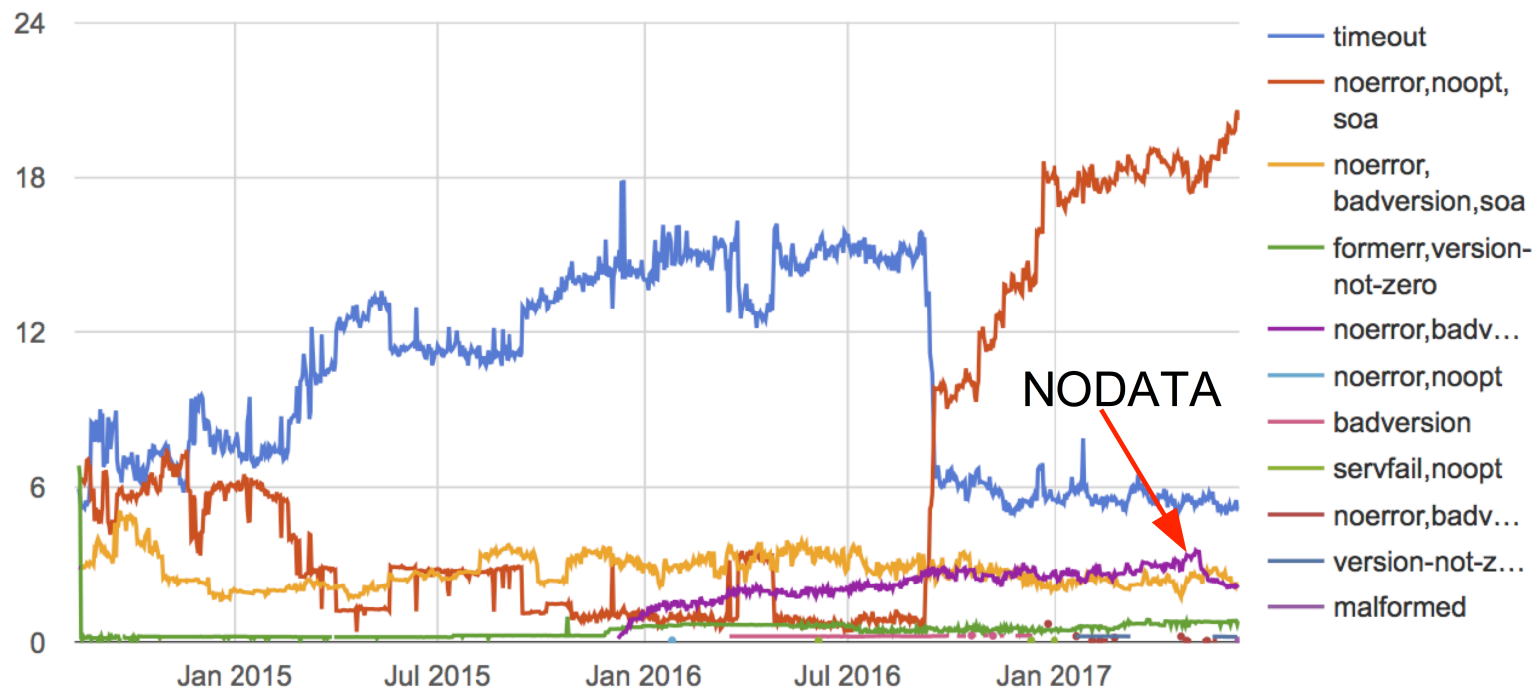
Alexa .GOV Servers EDNS(1) Failure Reasons



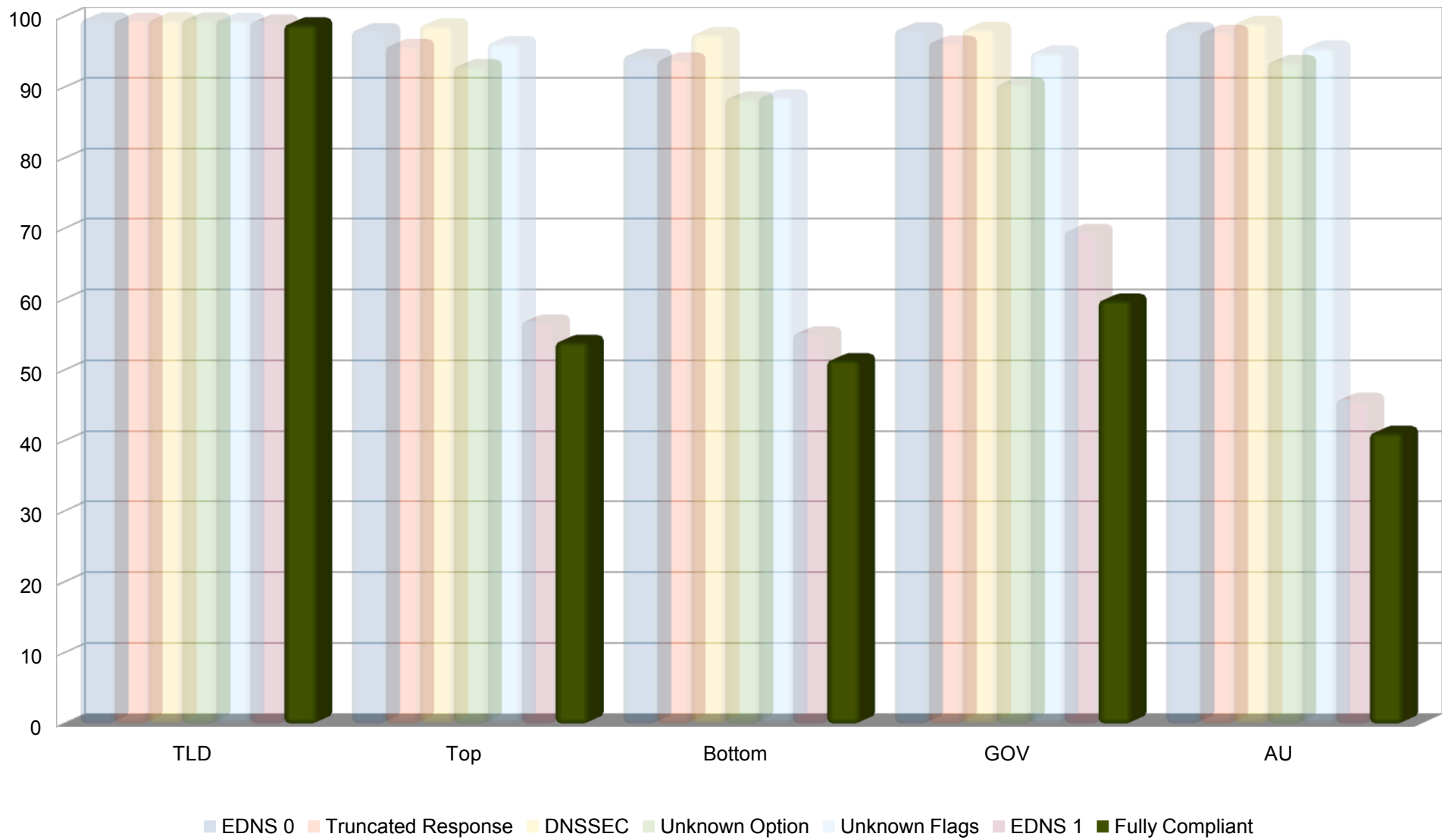
Alexa .GOV Servers EDNS(1) Failure Reasons



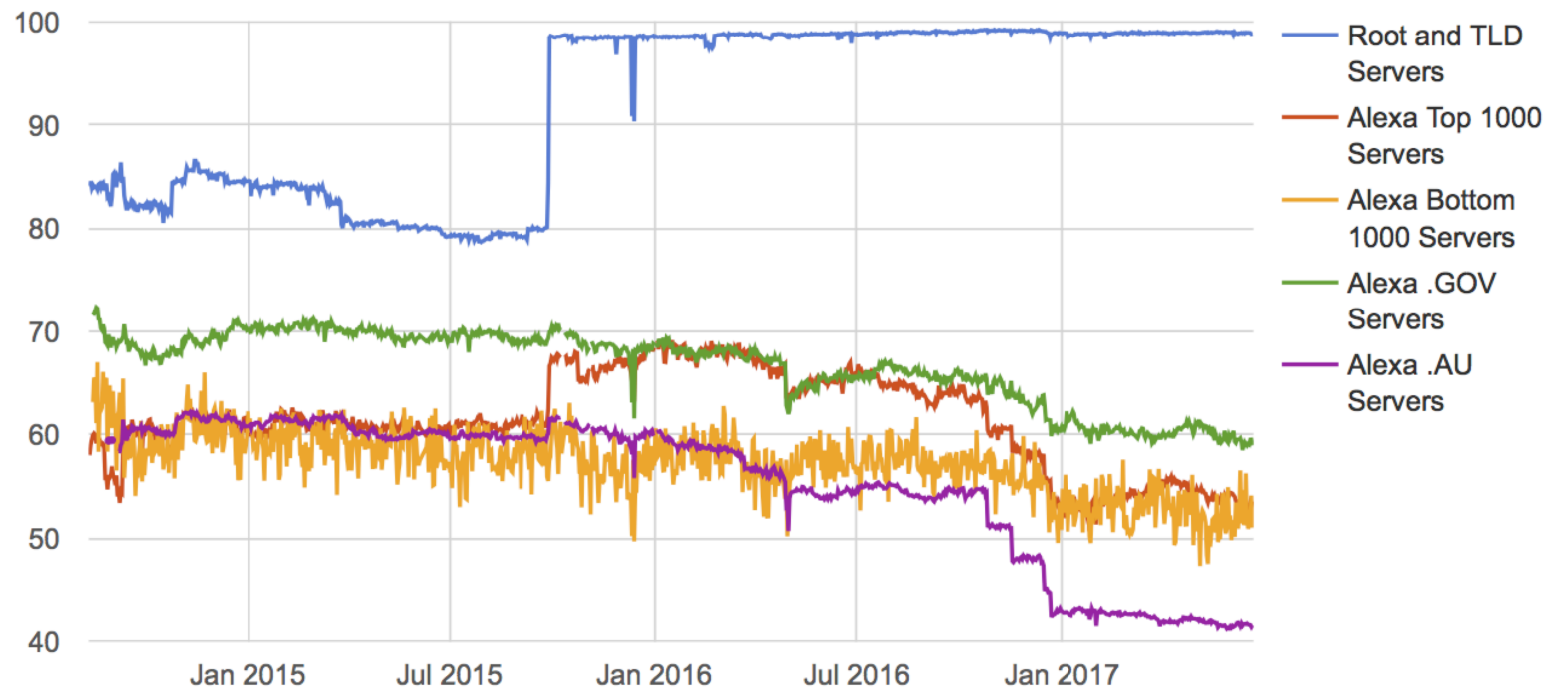
Alexa .GOV Servers EDNS(1) Failure Reasons



EDNS Compliance by Function of EDNS Aware Servers - 31 May 2017



Percentage of EDNS aware servers that passed all EDNS compliance tests



# Fixing Non-compliance

- Fix the DNS server implementations
- Fix firewall implementations
- Have agreed tests for non-compliance
- Introduce policy to say that non-compliant servers are not permitted.
- Introduce the new policy with grace period for existing servers
- Regularly test for compliance and remove delegations with non-complying servers

# Fixing Non-compliance

- Fix the DNS server implementations
- Fix firewall implementations
- Have agreed tests for non-compliance
- Introduce policy to say that non-compliant servers are not permitted.
- Introduce the new policy with grace periods for existing servers and initially warnings for new servers
- Regularly test for compliance and remove delegations with non-complying servers

# More Information

<https://ednscomp.isc.org/>

Test your own servers

<https://ednscomp.isc.org/ednscomp>

draft-ietf-dnsop-no-response-issue