DNSSEC Deployment in .GOV Progress and Issues

Rod Rasmussen

President & CTO, Internet Identity

rod.rasmussen@internetidentity.com

ACTIVELY SECURING THE EXTENDED ENTERPRISE

Background on .GOV space

- For use by US government entities
  - Federal, non-DOD
  - State and local governments can apply
  - Native American "nations" provisioned as well
- Inconsistent policy on naming standards
- Applicant rules "loose" and have changed
- No zone file published publicly (FOIA filing???)

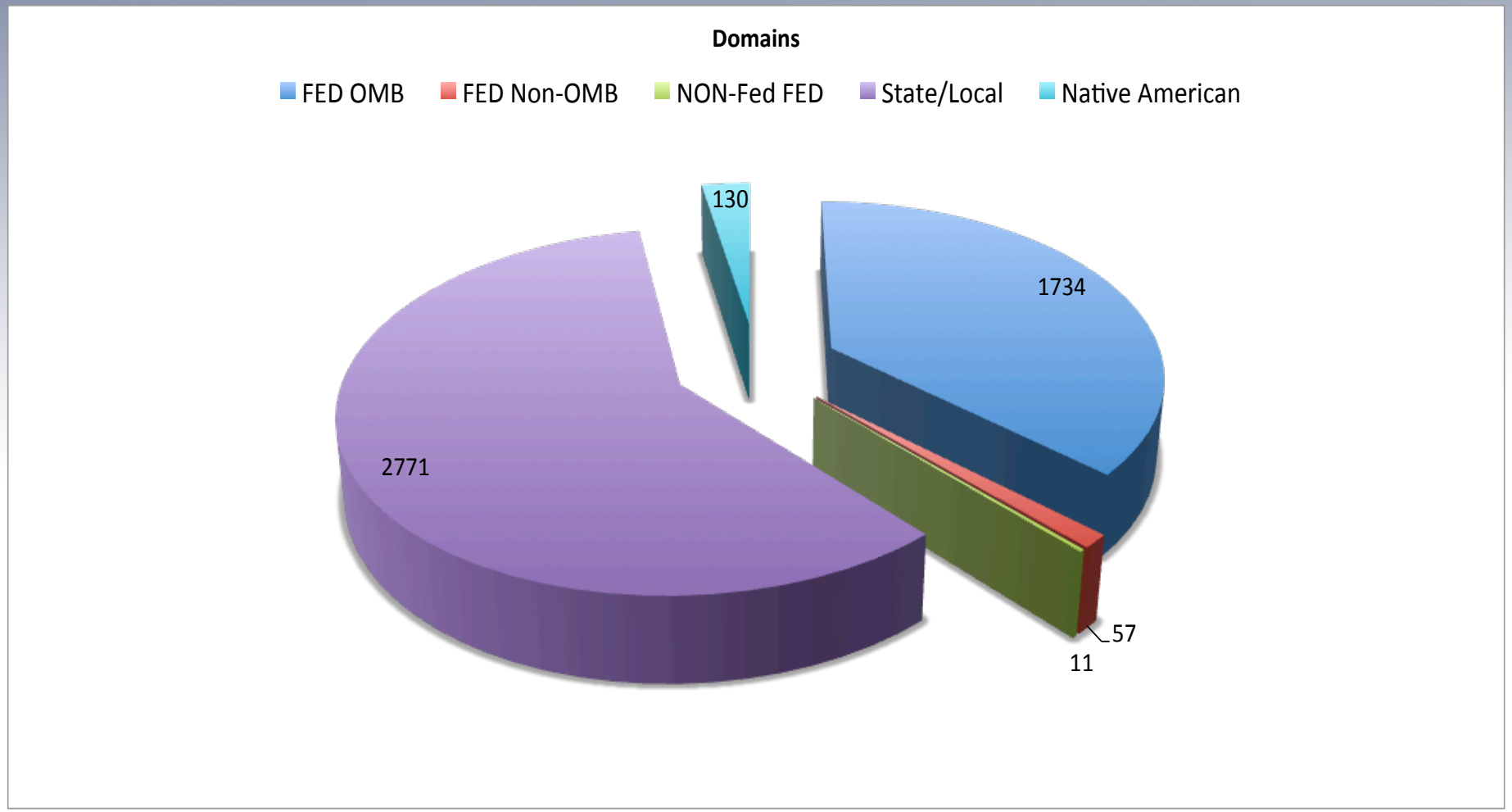
OMB Directive and Tracking

- In August 2008 OMB (Office of Management and Budget) directed that GOV zones be signed by January 2009
- Government to lead way in DNSSEC deployment
- Some major issues
  - Signing requirements not thorough (how?/SLA/maintenance)
  - Didn't apply to state/local/native American
  - Not all US federal entities come under OMB rules
- Penalties for non-compliance? Benefits for implementation?
- So we aren't there yet, have to measure the progress being made.

.GOV Zone Sizing

- Put together "pretty good" .gov zone file in 2010
  - Some publicly available, some from researchers
  - Passive DNS replication
  - Use of known GOV entities and checked for existence
- Found 2941 domains
- Report in 2010 led to friendly input from people with more data…
- This time we have high confidence in nearly entire zone
- Just over 4700 domains under registration in July 2011

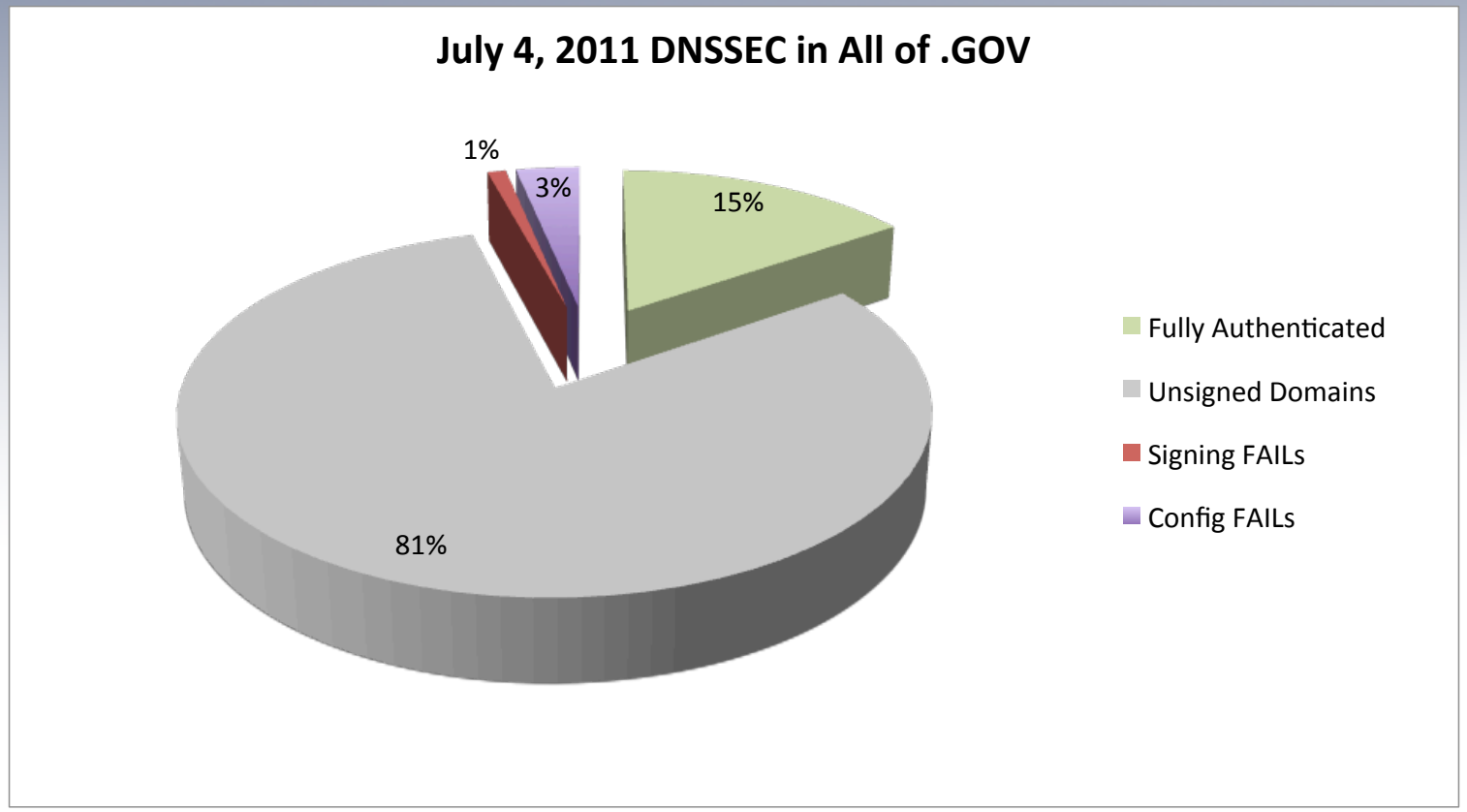
.GOV Zone Distribution



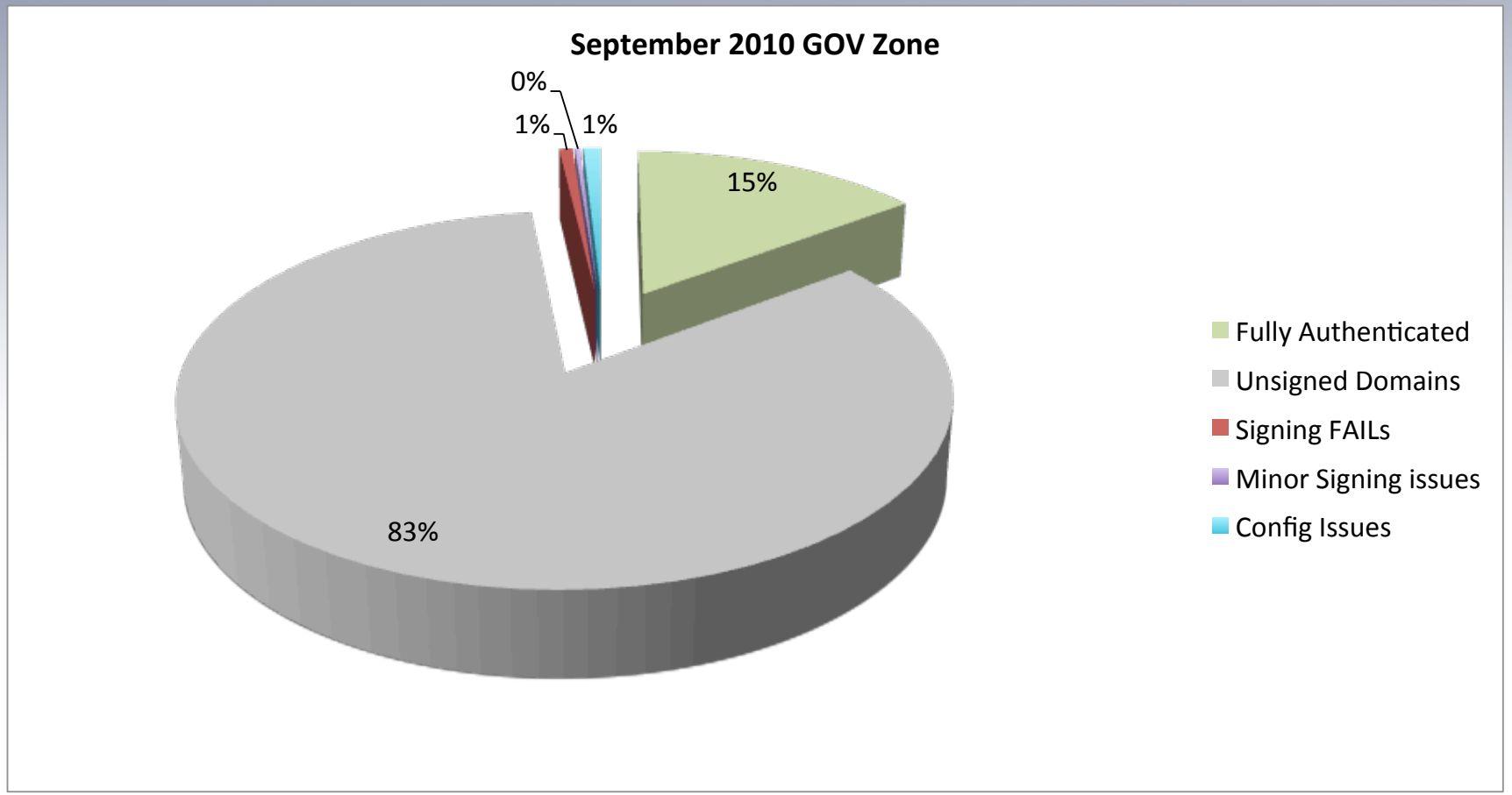
Study Methodology

- Walk the zone – digging for DNSSEC responses
  - Repeat for non-authenticated 2-3 times over day
  - Repeat every few minutes for DNSSEC error conditions
- Utilize DNS-OARC recursive DNSSEC validator servers
  - BIND 9 - 149.20.64.20
  - Unbound - 149.20.64.21
- Compare fails against non-DNSSEC aware recursives
  - Find general DNS failures (non-delegation, non-response, etc.)
- Tally results

Overall .GOV DNSSEC Deployment



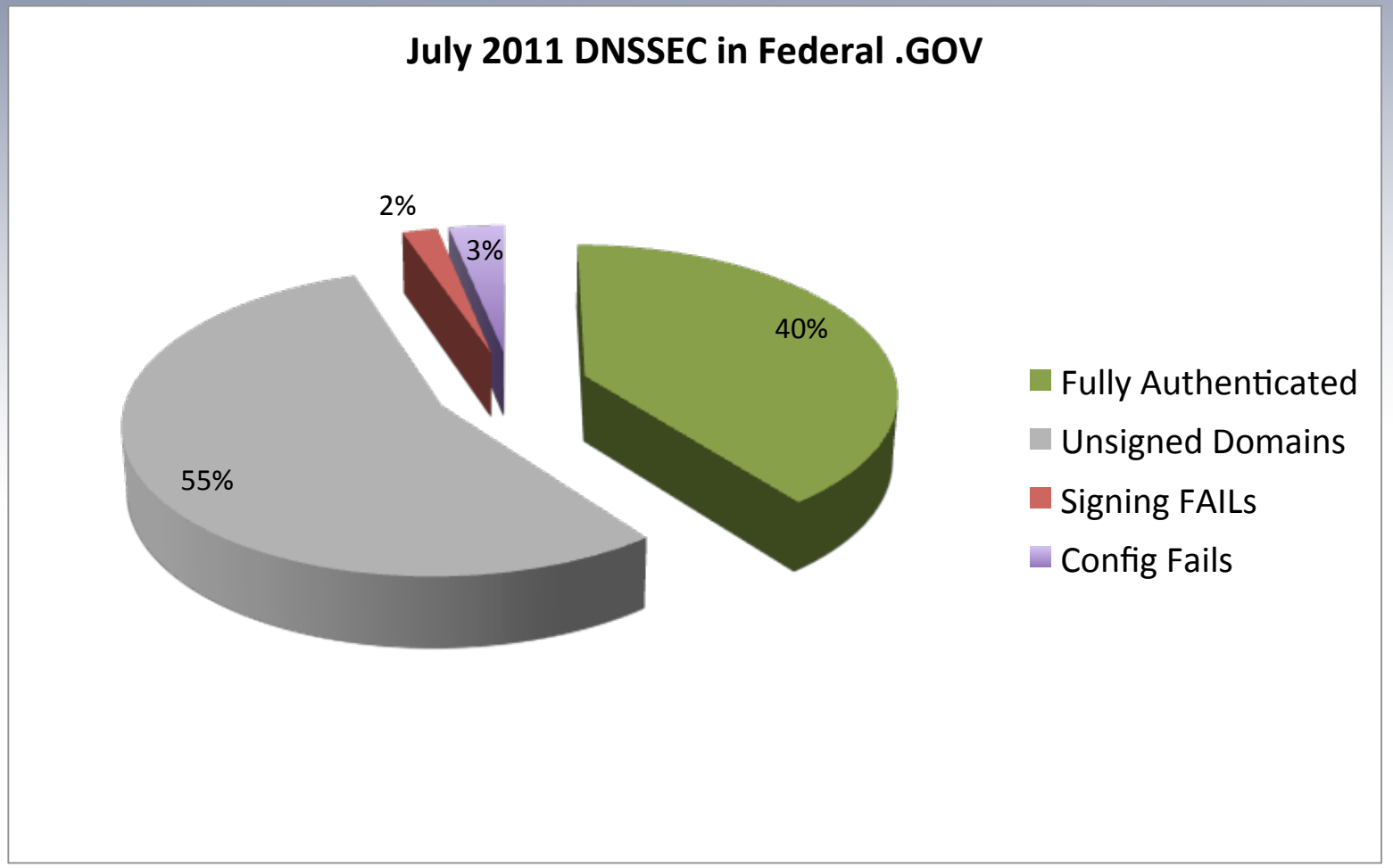
2010 Overall Findings



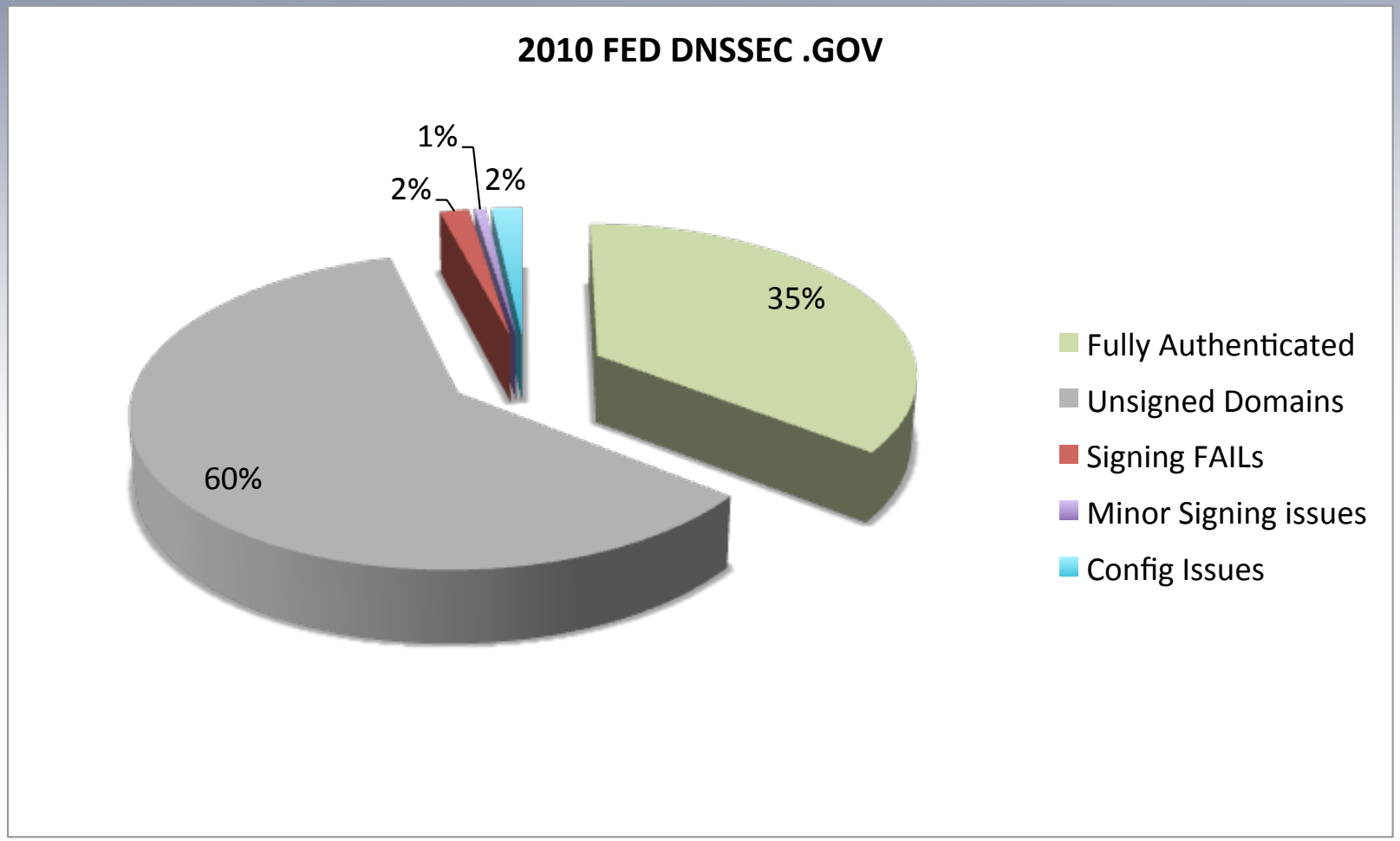
.GOV DNNSEC By the Numbers

Result	Number of Domains	Percentage
Fully Authenticated	723	15%
Unsigned	3781	80%
Signing FAIL	45	1%
Config FAIL	154	3%
Total Domains	4703	

DNSSEC for FED .GOV



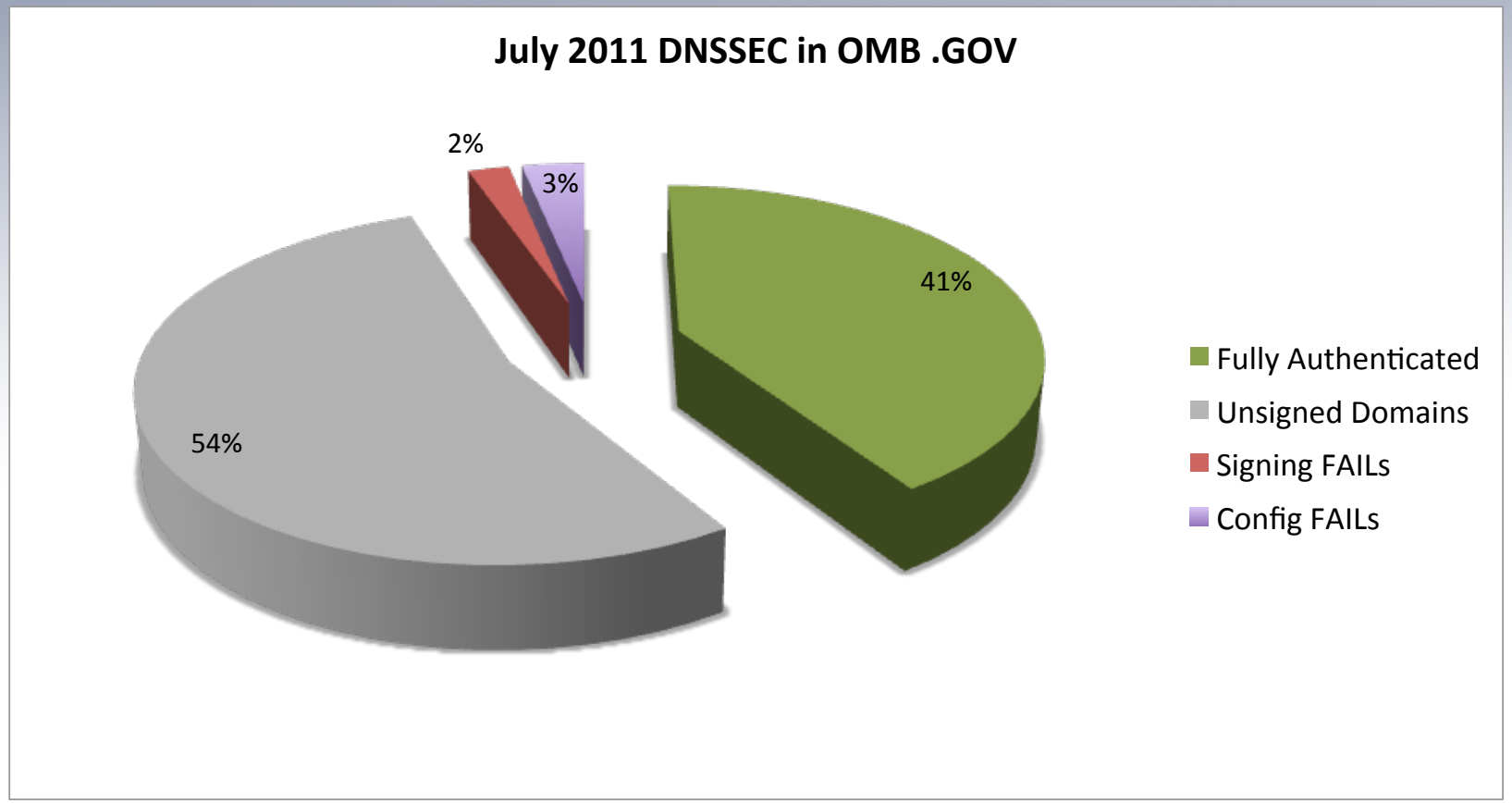
2010 DNSSEC for FED only GOV



Federal .GOV Numbers

Results	Domains	Share
Fully Authenticated	709	40%
Unsigned Domains	987	55%
Signing FAILs	37	2%
Config FAILs	58	3%
Total Domains	1791	

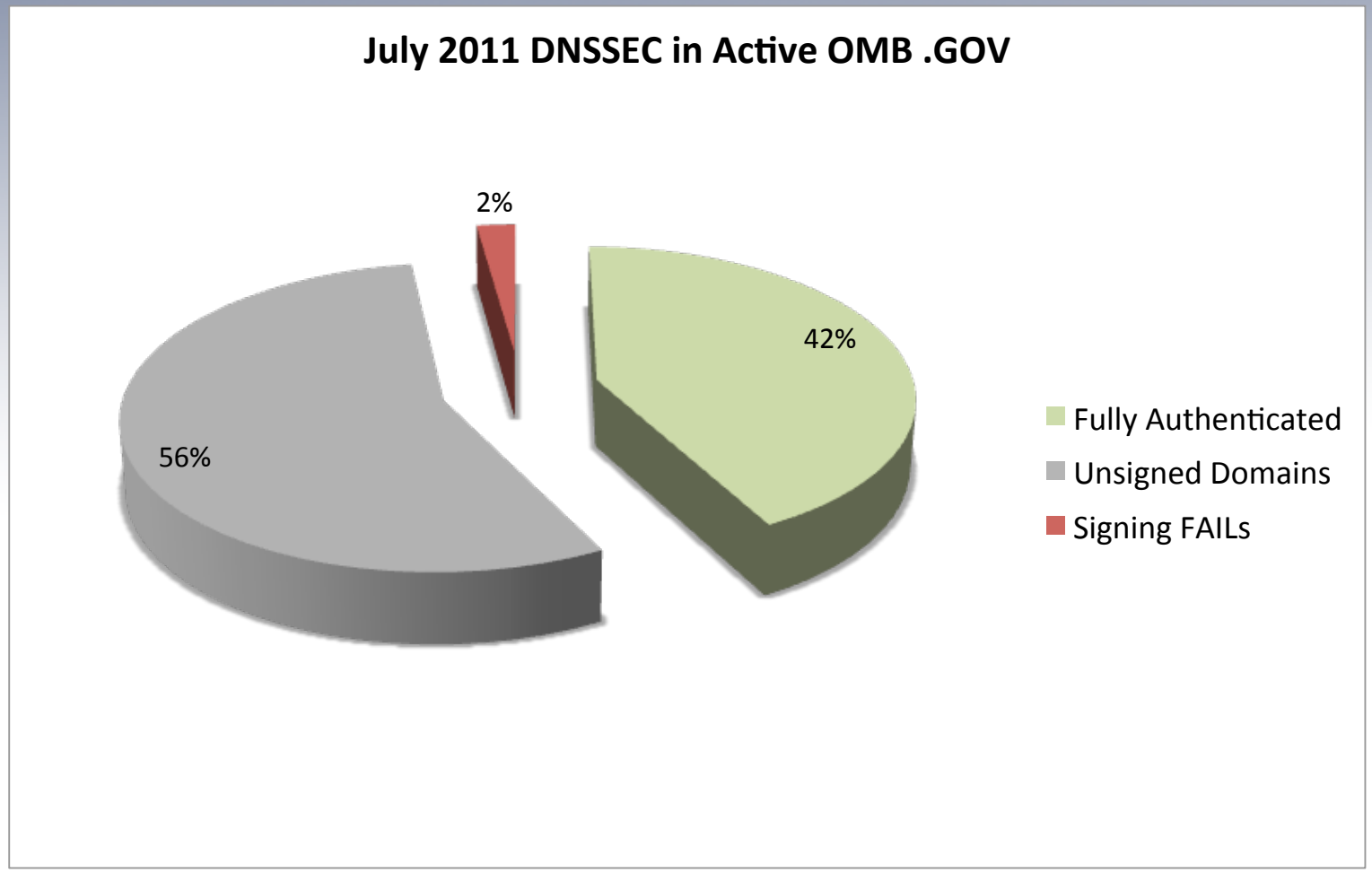
DNSSEC for FED under OMB



OMB Fed by the Numbers

Results	Domains	Share
Fully Authenticated	709	41%
Unsigned Domains	932	54%
Signing FAILs	37	2%
Config FAILs	56	3%
Total Domains	1734	

DNSSEC FED/OMB Active-only



DNS Issues in .GOV

- 154 domains not deployed properly
  - Not available from designated nameservers
  - Nameservers refuse to answer any queries at all
- 682 Domains have been deleted vs. what was expected
- 45 Signing failures of some sort that would lead all or some users unable to contact domain

DNSSEC FAIL Issues

- Most are BIND vs. Unbound config diffs
- Topic of discussion within the community?
- BIND authenticates. Unbound authenticates the DS RR but authentication fails for the domain records.
  - 39 out of 45
- No DS RR for the Domain. Unbound gives answers without AD bit, while BIND provides a SERVFAIL
  - 6 out of 45

Finishing Deployment

- Incentives/penalties within OMB GOV
- Figure out deployment problems and fix
- Non-OMB Fed needs pushing
- Mandate DNSSEC at renewal for states/local/tribes

Proper DNSSEC Maintenance

- How about a coordinated monitoring program by some federal agency?
  - Ignorance is probably bliss today
  - Requirements with teeth, incentives?
- BCP from providers and agencies that do well
- Input from ISPs (Comcast and other early US adopters)
- Make sure deployments work for all resolvers

Future work

- Outreach to state/local
- Look at near real-time monitoring and events rather than snapshots
- Deeper analysis of error conditions and recommendations for fixes
  - Partner up with other researchers
- Look at MIL when it rolls out
- Look at sensitive domains in com/net/org

DNSSEC Deployment in .GOV Progress and Issues

Thanks!

Rod Rasmussen

President & CTO, Internet Identity

rod.rasmussen@internetidentity.com

ACTIVELY SECURING THE EXTENDED ENTERPRISE