VOKE CYBER PRESENTS

DNS Security Posture Checklist

What to actually check, fix, and document against NIST SP 800-81r3

PUBLISHED	REFERENCE	AUTHOR
March 2026	NIST SP 800-81r3	Louis Sanchez

NIST published SP 800-81r3 on March 19, 2026, the first update to the federal DNS security guide in over 12 years. The philosophy behind it is a major shift: DNS is no longer just infrastructure to protect. It is an active security layer that should be protecting you. This guide gives you the practical version: six areas to check against the new standard, with clear actions and a prioritization framework.

1 Do You Have Protective DNS Deployed?

HIGHEST PRIORITY

Protective DNS (PDNS) is the biggest new addition to the guide. It is a DNS resolver with threat intelligence layered on top that blocks malicious domains in real time instead of resolving everything it is asked to. For federal agencies this is now an expected control. For everyone else, it is the direction auditors and insurers are heading.

- [ ] **Are your recursive resolvers filtering known-malicious domains?**
  Cloudflare Gateway, Cisco Umbrella, Infoblox, and NextDNS for Teams are common options.

- [ ] **Are DNS query logs being generated and retained?**
  Logs are required to support both PDNS and SIEM correlation requirements.

- [ ] **If no PDNS is deployed, is there a documented remediation plan?**
  This is your highest-priority gap against the new guidance.

ⓘ PDNS is the single highest-impact DNS control per dollar. If you deploy one thing from this checklist, make it this.

2 Audit Your Encrypted DNS Situation

VISIBILITY RISK

DoT, DoH, and DoQ are all formally covered now. For federal agencies, encrypted DNS is mandatory where technically feasible. For everyone else, it is the direction auditors and insurers are heading. The guide specifically calls out browser DoH bypass as a risk to manage.

- [ ] **Are clients resolving over encrypted DNS to internal resolvers?**
  DoT runs on TCP port 853. DoH runs on TCP/UDP port 443. DoQ on UDP port 853.

- [ ] **Are browsers silently bypassing your corporate resolver with DoH?**
  Chrome, Firefox, and Edge can use Google or Cloudflare DoH by default, killing your DNS visibility.

- [ ] **Is unauthorized DoT traffic on TCP port 853 blocked at the perimeter?**
  Blocking outbound port 853 forces clients to use your controlled resolver.

3 Audit Your DNSSEC Crypto

MODERNIZATION

If you have DNSSEC deployed, the algorithm question matters now. The guide prefers ECDSA and Edwards-curve algorithms over RSA because smaller key sizes keep DNS responses compact enough to avoid TCP fallback. Key rotation should be automated. Manual key management is the 2013 approach.

- [ ] **Are you signing with RSA/SHA-256, or migrated to ECDSA P-256 or Ed25519?**
  NIST SP 800-57 and RFC 8624 now recommend ECDSA and Edwards-curve algorithms.
- [ ] **Are RRSIG validity windows set to 5 to 7 days?**
  Anything measured in weeks is out of spec with the new guidance.
- [ ] **Is key rotation automated, and are key-signing keys stored in an HSM?**
  Manual key management on a calendar reminder is no longer acceptable practice.
- [ ] **If DNSSEC is not deployed, is there a deployment plan?**
  Most major registrars and DNS providers now support one-click DNSSEC signing.

4 Scan for Dangling DNS Records

IMMEDIATE RISK

Subdomain takeover via dangling CNAME records is now a formally documented threat in SP 800-81r3. First time NIST has addressed it explicitly. A CNAME pointing to a deprovisioned cloud resource is an open door for attackers to claim that subdomain.

- [ ] **Run subdomain enumeration and check every CNAME for liveness.**
  Any CNAME pointing to AWS, Azure, GitHub Pages, Heroku, or Fastly returning 404 is a takeover candidate.
- [ ] **Check for lame delegations: NS records pointing to nameservers you no longer control.**
  Lame delegations enable domain hijacking through a hosting provider.
- [ ] **Are retired domains being parked rather than allowed to expire?**
  Expired domains can be re-registered by attackers to take over delegations.
- [ ] **Is there active monitoring for look-alike and typosquat registrations?**
  SP 800-81r3 explicitly recommends monitoring for domain impersonation.

5 Get DNS Logs Into Your SIEM

DETECTION GAP

The new guide is explicit: DNS query logs should feed your SIEM and be correlated with DHCP lease history so you can map IP addresses to specific assets during incident response.

- [ ] **Are DNS query logs being generated at the resolver level?**
  Both authoritative and recursive resolvers should produce query logs.
- [ ] **Are those logs forwarding to your SIEM or log aggregation platform?**
  Integration with SIEM is now an explicit NIST recommendation.
- [ ] **Can you answer: what did this IP query for at 2am last Tuesday?**
  If the answer is no, your DNS layer is invisible to your SOC.
- [ ] **Is DNS query data correlated with DHCP lease history?**
  DHCP correlation maps IP addresses to named assets during investigations.

ⓘ Without DNS-to-DHCP correlation, you can see what was queried but not which device made the query. That gap makes incident response significantly harder.

6 Verify Your Architecture Still Holds

VALIDATION

The 2013 architectural recommendations are still valid. The 2026 guide kept them. But they are worth confirming, especially after cloud migrations that quietly break clean separation.

- [ ] **Are authoritative and recursive resolver functions separated?**
  Combining both functions on one internet-facing server is called out as a security risk.
- [ ] **At least two authoritative servers on separate network segments?**
  Geographic distribution across different physical sites is also recommended.
- [ ] **Is a hidden primary in use to reduce exposure to direct attack?**
  The hidden primary should not appear in the zone's NS record set.
- [ ] **Is zone transfer blocked to arbitrary external IPs?**
  Run: dig AXFR yourdomain.com @your-nameserver from an external IP to verify.

→ Quick Prioritization: Where to Start

If you are triaging where to start, here is the order that gets you the most risk reduction per dollar and per hour.

#	AREA	WHY FIRST
1	**Dangling Records**	Free to fix. Immediate risk reduction. No tooling required.
2	**Protective DNS**	Highest security impact per dollar of any DNS control.
3	**DNS Logs to SIEM**	Unlocks detection capability you currently cannot perform.
4	**Encrypted DNS Audit**	Stop the silent browser bypass problem killing your visibility.
5	**DNSSEC Crypto**	Important but lower urgency if DNSSEC is already deployed.
6	**Architecture Review**	Verify cloud migrations have not quietly broken separation.

"DNS is no longer something you protect. It is something you use to protect everything else."

Voke Cyber helps organizations understand their real attack surface, not just what a compliance checklist says. If your DNS posture has never been formally assessed, that is a conversation worth having.

Start a Conversation →

vokecyber.com
info@vokecyber.com

Full NIST SP 800-81r3:
csrc.nist.gov/pubs/sp/800/81/r3/final