DNS Intelligence Report

cisa.gov

2026-02-07 23:15 UTC · 0.4s

DNS & Trust Posture: **SECURE**

All security controls enforced including DNSSEC.

EMAIL SPOOFING	BRAND IMPERSONATION
Protected	Not Setup
DNS TAMPERING	**CERTIFICATE CONTROL**
Protected	Open

Configured

DMARC (email spoofing protection), DKIM (1 selector(s), 2048-bit), DNSSEC (DNS responses signed)

Not Configured

CAA (certificate authority control), MTA-STS (email TLS policy), TLS-RPT (TLS delivery reporting), BIMI (brand logo in inboxes)

REGISTRAR (RDAP)

get.gov

Where you pay to own domain

EMAIL SERVICE PROVIDER

Proofpoint

Where email is hosted (MX)

WEB HOSTING

Unknown

Where website is hosted

DNS HOSTING

Standard Gov Enterprise

Where DNS records are edited

Email Security

Can this domain be impersonated by email? **No**

Verdict: DMARC policy is reject - spoofed messages will be blocked by receiving servers. DKIM keys verified with strong cryptography (signed by Microsoft 365 via Proofpoint gateway).

SPF Record RFC 7208

Success -all 3/10 lookups

SPF valid with strict enforcement (-all), 3/10 lookups

```
v=spf1 include:spf.dhs.gov include:spf.protection.outlook.com include:spf-00376703.gpphosted.com -all
```

⚠ RFC 7489 §10.1: -all may cause rejection before DMARC evaluation, preventing DKIM from being checked

⚠ **SPF hard fail (-all): compliance-strong, but can short-circuit DMARC.** RFC 7489 §10.1 notes that -all can cause some receivers to reject mail during the SMTP transaction — before DKIM is checked and before DMARC can evaluate the result. A message that would pass DMARC via DKIM alignment may be rejected prematurely. For most domains, ~all + DMARC p=reject is the strongest compatible posture — it ensures every authentication method (SPF, DKIM, DMARC) is fully evaluated before a decision is made.

Federal compliance context: CISA BOD 18-01 requires valid SPF records for federal civilian agency domains. The directive doesn't explicitly specify -all vs ~all, but -all is widespread federal practice as defense-in-depth. This domain's use of -all follows that convention.

DMARC is set to reject — enforcement is strong. However, some receivers may still reject messages on SPF hard fail before DKIM alignment is checked.

SPF flattened by Proofpoint EFD (Gov) (Proofpoint)

DMARC Policy

RFC 7489

Success p=reject

DMARC policy reject (100%) - excellent protection

```
v=DMARC1; p=reject; pct=100; rua=mailto:DMARC@hq.dhs.gov, mailto:reports@dmarc.cyber.dhs.gov
```

Alignment: SPF relaxed DKIM relaxed

DKIM Records

RFC 6376

Found 2048-bit

Found DKIM for 1 selector(s) with strong keys (2048-bit)

> Mail routed through **Proofpoint** (security gateway) — DKIM signed by **Microsoft 365** (sending platform). This is a standard enterprise architecture.

selector1._domainkey Microsoft 365 2048-bit

```
v=DKIM1; k=rsa; p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAv32BRAJaAOsxAp31ZqQwd7RYfbYowvb3F7lq8WQEyasI6w7Gm0bxPW57TFM04fM5flf1PYyCDSa3ckQzSQLYmMx9HiXYJYF1Dpk9PnjTarbdR9mm9fc7iBXT2pTFNJw+SRMH3NRrbkefv8GqqLdJotgCl2vWoyRlfKCANCFq5Bbq4qaztXqU/cHRurG8ZVSF7ZrhY4EBKvpzAyIisrf2g2Gky+vO4LTMrgZeNnA/OyHmWmvlUC58e06jBLSysYyh19O4MiU5eUhuT7MYTLWz6fIOl4PaT9HkmM0rH/fgcGSYc8ajCsrvxYA8LgoWR9IzYq5vYzDWLxSo/J0c+6pVWQIDAQAB;
```

MTA-STS

RFC 8461 Warning

No MTA-STS record found

TLS-RPT RFC 8460 Warning

No TLS-RPT record found

Email Security Management Actively Managed

Intelligence: This domain uses dedicated email security management — indicating continuous monitoring and professional oversight, not a "set and forget" configuration. Most tools ignore reporting destinations; we extract the operational security partner network directly from DNS.

Proofpoint EFD (Gov) by Proofpoint

SPF flattening

SPF flattening (include:spf-00376703.gpphosted.com)

SPF flattening detected: Dynamic SPF management via Proofpoint EFD (Gov) — keeps include count within the 10-lookup limit automatically.

Brand Security

Can this brand be convincingly faked? Partially

Verdict: No brand protection controls - attackers could obtain certificates or impersonate visually.

BIMI BIMI Spec Warning

No BIMI record found

CAA RFC 8659 Warning

No CAA records found - any CA can issue certificates

Domain Security

Can DNS itself be tampered with? **No**

Verdict: DNS responses are authenticated from the root downward. Delegation is verified.

DNSSEC

RFC 4033 **Signed** **ECDSA P-256/SHA-256**

DNSSEC fully configured and validated - AD flag confirmed by resolver

Chain of trust: Root → TLD → Domain. DNS responses are authenticated and tamper-proof.

AD Flag: **Validated** - Resolver (8.8.8.8) confirmed cryptographic signatures

DS Record (at registrar):

```
2371 13 2 5F15E517D7A353D755D9D3F8548A3475CE88A738E62B766F5E33CFC4163AB934
```

NS Delegation

Verified

3 nameserver(s) configured

Nameservers:

blue.foundationdns.com blue.foundationdns.net blue.foundationdns.org

Multi-Resolver Verification: Discrepancy detected - Some resolvers returned different results

(1 difference found)

Resolver Differences:

A: Quad9 returned different results: ['184.27.230.106']

This may indicate DNS propagation in progress or geo-based DNS routing.

Traffic & Routing

Where traffic flows & how services resolve

A IPv4 Address

```
23.4.61.38
```

Where the domain points for web traffic

AAAA IPv6 Address

```
2600:1407:3c00:a83::3ff9
```

```
2600:1407:3c00:a93::3ff9
```

IPv6 ready

MX Mail Servers

```
10 mxa-00376703.gslb.gpphosted.com.
```

```
10 mxb-00376703.gslb.gpphosted.com.
```

Priority + mail server for email delivery

SRV Services

```
_sipfederationtls._tcp: 100 3600 5061 sipfed.online.lync.com.
```

SIP, XMPP, or other service endpoints

Web: Reachable (1 IPv4, 2 IPv6) **Mail:** 2 servers **Services:** 1 endpoint

Δ Changes Detected: A AAAA Resolver ≠ Authoritative (TTL / CDN rotation / recent change)

Risk: Low - typically resolves within TTL

Live DNS Diff

Real-time propagation comparison | See exactly what public resolvers return vs. what your authoritative nameserver has. Spot propagation delays, stale cache, and DNS misconfigurations instantly.

DNS Evidence Diff Side-by-side comparison

Resolver Records (Public DNS cache)

Authoritative Records (Source of truth)

A — Propagating — 1 / 1 records

Resolver Records	Authoritative Records
23.4.61.38	
	23.64.138.233

AAAA — Propagating — 2 / 2 records

Resolver Records	Authoritative Records
2600:1407:3c00:a83::3ff9	
	2600:1404:ec00:128b::3ff9
2600:1407:3c00:a93::3ff9	
	2600:1404:ec00:128c::3ff9

MX — Synchronized — 2 / 2 records

Resolver Records	Authoritative Records
10 mxa-00376703.gslb.gpphosted.com.	
	10 mxa-00376703.gslb.gpphosted.com.
10 mxb-00376703.gslb.gpphosted.com.	
	10 mxb-00376703.gslb.gpphosted.com.

TXT — Synchronized — 10 / 10 records

Resolver Records	Authoritative Records
_e01yoinuk3n6xrtnc8q3m9bdjyihdd7	
	MS=ms36056523
adobe-idp-site-verification=edfd88b4c2bdf65395c78b55da3580466eefa9aa874d5bcfb853692813e80515	
	MS=ms41452370
google-site-verification=BNRBfY90BM54Mf_pgL4Eg07IkwbGvq5nsdZCOYadDlM	
	MS=ms53160703

f188eb27-a746-4aa8-b160-eb68b0aab05d

_e01yoinuk3n6xrtnc8q3m9bdjyihdd7

MS=ms36056523

_tufdw17aa2wht723upz8w56htpvpgkw

v=spf1 include:spf.dhs.gov include:spf.protection.outlook.com include:spf-00376703.gpphosted.com -all

adobe-idp-site-verification=edfd88b4c2bdf65395c78b55da3580466eefa9aa874d5bcfb853692813e80515

google-site-verification=wsLVyeZYgv0NLikdmfm2m3XPP-986Ylo8XxUkrjIOvA

f188eb27-a746-4aa8-b160-eb68b0aab05d

MS=ms41452370

google-site-verification=BNRBfY90BM54Mf_pgL4Eg07IkwbGvq5nsdZCOYadDlM

MS=ms53160703

google-site-verification=wsLVyeZYgv0NLikdmfm2m3XPP-986Ylo8XxUkrjIOvA

_tufdw17aa2wht723upz8w56htpvpgkw

v=spf1 include:spf.dhs.gov include:spf.protection.outlook.com include:spf-00376703.gpphosted.com -all

NS Synchronized 3 / 3 records

blue.foundationdns.org.

blue.foundationdns.com.

blue.foundationdns.net.

blue.foundationdns.net.

blue.foundationdns.com.

blue.foundationdns.org.

SRV 1 / 0 records

_sipfederationtls._tcp: 100 3600 5061 sipfed.online.lync.com.

–

Confirm Your Email Configuration

This tool analyzes DNS records, but to verify actual email delivery, send a test email to Red Sift Investigate. Their tool shows exactly how your emails arrive, including SPF/DKIM/DMARC pass/fail results in the headers.

Report reflects evaluated DNS security posture at time of generation.

Made by IT Help San Diego Inc.

Need help with DNS? Call 619-853-5008