DNS Intelligence Report

cia.gov

DNS & Trust Posture: **SECURE (Monitoring)**

Security controls present but some in monitoring mode.

1 monitoring

Analyzed: 2026-02-07 03:36 UTC Duration: 0.6s

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

Monitoring
DMARC quarantine (p=reject recommended for full enforcement)

Configured
DKIM (1 selector(s), 2048-bit), DNSSEC (DNS responses signed), CAA (certificate issuance restricted)

Not Configured
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
Cia.Gov
Where email is hosted (MX)

WEB HOSTING
Akamai Edge DNS
Where website is hosted

DNS HOSTING
Akamai Edge DNS Gov Enterprise
Where DNS records are edited

Email Security

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

Verdict: DMARC policy is quarantine - spoofed messages will be flagged as spam. DKIM keys

verified with strong cryptography.

SPF Record

RFC 7208

Success -all 1/10 lookups

SPF valid with strict enforcement (-all), 1/10 lookups

```
v=spf1 mx -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 mandates -all for federal civilian agency domains. This domain's use of -all is compliant with that directive. **DMARC enforcement is partial (quarantine). -all may preempt DKIM/DMARC**

DMARC Policy

RFC 7489

Success p=quarantine

DMARC policy quarantine (100%) - good protection

```
v=DMARC1; p=quarantine;
sp=quarantine; pct=100;
rua=mailto:demarcreport
s@uce.cia.gov; ruf=mailt
o:demarcfailures@uce.ci
a.gov; ri=86400; aspf=s;
adkim=s; fo=1
```

Alignment: SPF strict DKIM strict sp=quarantine

⚠ Forensic reports (ruf) configured - many providers ignore these

DKIM Records

RFC 6376

Found 2048-bit

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

✓ s1._domainkey 2048-bit

```
v=DKIM1; p=MIGfMA0GCSqGS
Ib3DQEBAQUAA4GNADCBiQKBg
QDWKDG6o+aUX3ov7h3zsv1mj
Q5oTy8kFUYXMtgRQxrk3BHfM
7cEXysehX3MaOgf/1JuN1dzm
bwTMG9WqY1ikhQTjWbi0qVP0
LMw7QSXmkdpmGl/QXEKp5LJD
NGTuE3yPtD/068WPe1wYI2Oq
x/ODOkxF4LUx7tbhjBBgzXtl
8/Z5QIDAQAB;
```

evaluation at some receivers. Consider p=reject for full enforcement; ~all is more DMARC-compatible.

MTA-STS RFC 8461 Warning

No MTA-STS record found

TLS-RPT RFC 8460 Warning

No TLS-RPT record found

Brand Security

Can this brand be convincingly faked? No

Verdict: Certificate issuance is controlled but brand logo (BIMI) is not configured.

BIMI BIMI Spec Warning

No BIMI record found

CAA RFC 8659 Success IODEF

CAA configured - only DigiCert can issue certificates

Authorized CAs: DigiCert

```
0 iodef "mailto:caanotices@uce.cia.gov"
```

```
0 issue "digicert.com"
```

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 | RSA/SHA-25

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):

```
48959 8 2 DEB2A237884DDCFD20BDFF8E8FA81F4A
4B7ED069E1E4E2ED79CAE7707D1CFFFC
```

```
1015 8 2 66B64EA16CD54EEC14BDEF2ECA16E1BCC
62A2DD7A95FE64A24CBAF2A7E411436
```

```
62599 8 2 E51AE54018E41619F97076A56C969D10
A71B4D0050DBF1E6AB8DE2F8CF023AE5
```

NS Delegation

Verified

6 nameserver(s) configured

Nameservers:

- a1-22.akam.net
- a12-65.akam.net
- a13-65.akam.net
- a16-67.akam.net
- a22-66.akam.net
- a3-64.akam.net

Multi-Resolver Verification: Discrepancy detected - Some resolvers returned different results (2 differences found)

Resolver Differences:

- A: Quad9 returned different results: ['23.211.124.239', '23.211.124.240']
- A: Cloudflare returned different results: ['23.64.114.71', '23.64.114.72']

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

Traffic & Routing

Where traffic flows & how services resolve

A IPv4 Address

184.25.148.152

184.25.148.193

Where the domain points for web traffic

AAAA IPv6 Address

2600:1401:2000::b819:94c1

2600:1401:2000::b819:9498

✓ IPv6 ready

MX Mail Servers

10 mail3.cia.gov.

10 mail4.cia.gov.

Priority + mail server for email delivery

SRV Services

— No SRV records

No service-specific routing configured

Web: Reachable (2 IPv4, 2 IPv6) **Mail:** 2 servers **Services:** None

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	2 / 2 records
184.25.148.152	23.195.81.155
184.25.148.193	23.195.81.144
AAAA Propagating	2 / 2 records
2600:1401:2000::b819:94c1	2600:1406:2e00:20::45c0:8bc5
2600:1401:2000::b819:9498	2600:1406:2e00:20::45c0:8bdd
MX Synchronized	2 / 2 records
10 mail3.cia.gov.	10 mail4.cia.gov.
10 mail4.cia.gov.	10 mail3.cia.gov.
TXT Synchronized	1 / 1 records
v=spf1 mx -all	v=spf1 mx -all
NS Synchronized	6 / 6 records
a3-64.akam.net.	a16-67.akam.net.
a22-66.akam.net.	a1-22.akam.net.
a12-65.akam.net.	a12-65.akam.net.
a1-22.akam.net.	a3-64.akam.net.
a16-67.akam.net.	a22-66.akam.net.
a13-65.akam.net.	a13-65.akam.net.

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