YesGov

GOVERNMENT DOMAIN SECURITY REPORT

fresnofloodcontrol.org

Fresno Metropolitan Flood Control District, California

Checked September 28, 2026 at 5:52 PM UTC · Check ID 0916ec7c-6dbb-4f60-8a27-d5bb5d2bdbdd

C+

9 of 16 checks passed **Needs attention**

The basics are in place, but several standard protections are missing. The list below is in order of risk to residents.



9 passed · 1 needs attention · 6 missing

Website	Email	DNS and domain
2 of 8	4 of 5	3 of 3

Not on a .gov domain

fresnofloodcontrol.org is not a .gov address. Anyone can register a look-alike .com or .org, so residents cannot tell from the address alone that this is the official site.

CISA and DHS advise that .gov is a requirement for secure government, trusted communication and public trust. Every day on a non-.gov address is a day residents can be fooled by an impostor site or email.

What to fix first

In order of risk to residents. Each is a one-time setting that then needs to be watched.

1. **Send every visitor to HTTPS** — HIGH RISK
   Residents who type the plain address or follow an old link get an unencrypted page that can be read or changed on public Wi-Fi.
   Fixed by: Your web host

2. **Turn on HSTS** — MEDIUM
   On public Wi-Fi, a resident's visit can be pushed to an unencrypted copy of the site.
   Fixed by: Your web host

3. **Enforce MTA-STS** — MEDIUM
   MTA-STS is set up but not enforced, so mail to agency staff can still be forced onto an unencrypted connection.
   Fixed by: Your email or DNS provider

4 **Add framing protection** MEDIUM

The site can be hidden inside a hostile page to trick residents into clicking buttons they cannot see.

Fixed by: Your web host

5 **Add a CAA record** MEDIUM

Any certificate authority in the world may issue a certificate for this domain, which makes impersonating the site easier.

Fixed by: Your DNS provider

6 **Add file type protection** MEDIUM

Browsers may guess file types, which can let an uploaded file run as code against visitors.

Fixed by: Your web host

7 **Publish a security contact (security.txt)** MEDIUM

People who find a security problem have no standard way to tell the agency before it is misused.

Fixed by: Your web host

All results in detail

Every record and value we saw, grouped by area. Written for your IT team, readable by anyone.

Website — 2 of 8 passed

HTTPS certificate — PASS

Issued by	**WE1**
Issued to	**fresnofloodcontrol.org**
Expires	**December 11, 2026 (73 days after this check)**
TLS version	**TLSv1.3**

Redirect to HTTPS — MISSING

HTTPS available	**No**
Plain address redirects to HTTPS	**No**

What this means: Residents who type the plain address or follow an old link get an unencrypted page that can be read or changed on public Wi-Fi.

How to fix: Redirect every http:// request to https:// with a permanent (301) redirect. (Your web host)

HSTS — MISSING

HSTS header	**Not sent**

What this means: On public Wi-Fi, a resident's visit can be pushed to an unencrypted copy of the site.

How to fix: Send the Strict-Transport-Security header with a max-age of at least one year. (Your web host)

Certificate trust and match — PASS

Trusted chain	Yes
Strong public key	Yes
Valid signature	Yes
Name matches domain	Yes

CAA record — MISSING

CAA record	Not found

What this means: Any certificate authority in the world may issue a certificate for this domain, which makes impersonating the site easier.

How to fix: Publish a CAA record naming the authority you use, for example 0 issue "letsencrypt.org". (Your DNS provider)

Framing protection — MISSING

X-Frame-Options	Not sent

What this means: The site can be hidden inside a hostile page to trick residents into clicking buttons they cannot see.

How to fix: Send the header X-Frame-Options: SAMEORIGIN, or a Content-Security-Policy with frame-ancestors 'self'. (Your web host)

File type protection — MISSING

X-Content-Type-Options	Not sent

What this means: Browsers may guess file types, which can let an uploaded file run as code against visitors.

How to fix: Send the header X-Content-Type-Options: nosniff. (Your web host)

Security contact (security.txt) — MISSING

/.well-known/security.txt	Not found

What this means: People who find a security problem have no standard way to tell the agency before it is misused.

How to fix: Publish /.well-known/security.txt with a contact address and an expiry date. (Your web host)

Email — 4 of 5 passed

SPF — PASS

Record	`v=spf1 ip4:4.16.41.216/29 include:spf.protection.outlook.com ip4:75.37.56.48/28 ip4:198.0.226.184/29 -all`
Ending	Strict (-all)

DKIM — PASS

Selectors found	selector1, selector2

DMARC — PASS

Policy	reject
Reports sent to	61b93c1fb310e@ag.dmarcly.com
Record	`v=DMARC1; p=reject; rua=mailto:61b93c1fb310e@ag.dmarcly.com; ruf=mailto:61b93c1fb310e@fo.dmarcly.com; sp=reject; pct=100; fo=1;`

MTA-STS — NEEDS ATTENTION

DNS record	Found
Policy file	Not found
Enforced	No

What this means: MTA-STS is set up but not enforced, so mail to agency staff can still be forced onto an unencrypted connection.

How to fix: Fix any problems listed for the policy file, publish the _mta-sts TXT record, and set the policy mode to enforce. (Your email or DNS provider)

TLS-RPT — PASS

Record	`v=TLSRPTv1; rua=mailto:61b93c1fb310e@tls.dmarcly.com`

DNS and domain — 3 of 3 passed

DNSSEC — PASS

Zone signed	Yes
Result	DNSKEY records found

IPv6 — PASS

Website reachable over IPv6	Yes
Website IPv6 addresses	2606:4700:3037::ac43:d459, 2606:4700:3034::6815:17a8
Name servers reachable over IPv6	Yes

RPKI route protection — PASS

Website route signed	Yes
Website route valid	Yes
Name server route valid	Yes

.gov domain — NOT SCORED

Ends in .gov	No

What this means: Anyone can register a look-alike .com or .org, so residents have no way to confirm this is the official site. Every .gov request is verified by CISA.

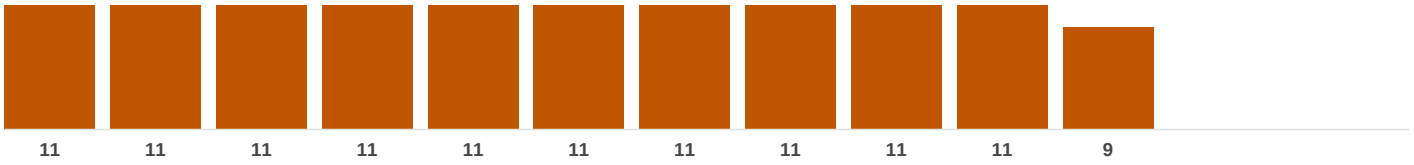
Hosting and platform

Informational, not scored

Website server	**172.67.212.89**
Mail server	**fresnofloodcontrol-org.mail.protection.outlook.com**
Website server reputation	**Not on abuse lists**
Mail server blocklists	**Not listed**
WordPress	**Not detected**
Email addresses published on the site	**0**
Broken links found	**0**
Referrer policy header	**No**

Progress over time

Checks passed at each scan, oldest to newest. Highest possible is 16.



If these basics were missed, what else has been missed?

These are published CISA standards that any IT department or provider can check in seconds. YesGov can fix all 7 in under 24 hours, re-run this check to prove it, and keep watching every day. The move to .gov takes 1 to 2 weeks because CISA verifies each request; security fixes on the current domain do not wait for it.

yesgov.com/contact · (888) 777-0017 · info@yesgov.com

How we check

We only check settings that any computer on the internet can see: DNS records, certificates, web headers and mail policies. We never log in to, scan or probe any agency system. The 16 checks build on CISA Binding Operational Directive 18-01 and other published internet standards. Full method: yesgov.com/open-data#how-we-grade.

Verify this report online

Scan the code or visit the address below to see these results, check the domain again and get alerts when anything changes.

https://yesgov.com/check/fresnofloodcontrol--org?check=0916ec7c-6dbb-4f60-8a27-d5bb5d2bdbdd

YesGov PBC is a Public Benefit Corporation that works only with U.S. government agencies. 1639 Medical Center Parkway, Murfreesboro, TN 37129. This report reflects public settings at the time of the check and is not a full security audit.