YesGov

GOVERNMENT DOMAIN SECURITY REPORT

# gsfahome.org

Golden State Finance Authority, California

Checked September 24, 2026 at 7:19 AM UTC · Check ID eae31ef0-9bdd-45ab-ad0b-e53d5c3df8c2

**D+**

**6** of 16 checks passed **Residents are exposed**

Basic protections recommended by CISA are missing. Each fix below is a standard setting, listed in order of risk to residents.



● 6 passed ● 1 needs attention ● 9 missing

| Website | Email | DNS and domain |
|---|---|---|
| 2 of 8 | 2 of 5 | 2 of 3 |

### Not on a .gov domain

gsfahome.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 DMARC enforcement on** — HIGH RISK
   A DMARC record exists but only monitors. Fake tax bills, utility shut-off notices and payment requests sent in the agency's name are still delivered.
   **Fixed by: Your email or DNS provider**

3. **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**

4 **Require encrypted mail delivery (MTA-STS)** MEDIUM
Mail sent to agency staff can be forced onto an unencrypted connection and read in transit.
**Fixed by: Your email or DNS provider**

5 **Turn on mail encryption reports (TLS-RPT)** MEDIUM
Nobody is told when encrypted mail delivery to the agency fails or is tampered with.
**Fixed by: Your DNS provider**

6 **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**

7 **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**

8 **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**

9 **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**

10 **Add IPv6 support** MEDIUM
Networks that only use IPv6, including some mobile carriers, cannot reach the site directly.
**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 | **GeoTrust TLS RSA CA G1** |
| Issued to | **gsfahome.org** |
| Expires | **December 11, 2026 (78 days after this check)** |
| TLS version | **TLSv1.3** |

## Redirect to HTTPS — MISSING

| | |
|---|---|
| HTTPS available | Yes |
| 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 2 of 5 passed

### SPF PASS

| | |
|---|---|
| Record | `v=spf1 include:spf.protection.outlook.com include:spfa.cpmails.com -all` |
| Ending | Strict (-all) |

### DKIM PASS

| | |
|---|---|
| Selectors found | selector1 |

### DMARC NEEDS ATTENTION

| | |
|---|---|
| Policy | none (monitor only) |
| Reports sent to | rcrcnet@us.cp-dmarc.com |
| Record | `v=DMARC1; p=none; rf=afrf; sp=none; fo=1; adkim=r; aspf=r; ruf=mailto:rcrcnet@us.cp-dmarc.com; rua=mailto:rcrcnet@us.cp-dmarc.com;` |

**What this means:** A DMARC record exists but only monitors. Fake tax bills, utility shut-off notices and payment requests sent in the agency's name are still delivered.

**How to fix:** After reviewing the reports, change p=none to p=quarantine, then to p=reject. (Your email or DNS provider)

### MTA-STS MISSING

| | |
|---|---|
| DNS record | Not found |
| Policy file | Not found |
| Enforced | No |

**What this means:** Mail sent to agency staff can be forced onto an unencrypted connection and read in transit.

**How to fix:** Publish an _mta-sts TXT record and a policy file at mta-sts.(domain)/.well-known/mta-sts.txt. (Your email or DNS provider)

### TLS-RPT MISSING

| | |
|---|---|
| TLS-RPT record | Not found |

**What this means:** Nobody is told when encrypted mail delivery to the agency fails or is tampered with.

**How to fix:** Publish a TXT record at _smtp._tls with an address to receive reports. (Your DNS provider)

## DNS and domain 2 of 3 passed

### DNSSEC PASS

| | |
|---|---|
| Zone signed | Yes |
| Result | DNSKEY records found |

### IPv6 MISSING

| | |
|---|---|
| Website reachable over IPv6 | No |
| Name servers reachable over IPv6 | No |

**What this means:** Networks that only use IPv6, including some mobile carriers, cannot reach the site directly.

**How to fix:** Ask the host for an IPv6 address and publish an AAAA record for the site. (Your web host)

## 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 | **40.112.243.51** |
| Mail server | **gsfahome-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 10 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/gsfahome--org?check=eae31ef0-9bdd-45ab-ad0b-e53d5c3df8c2

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.