YesGov

GOVERNMENT DOMAIN SECURITY REPORT

# flypib.com

Hattiesburg-Laurel Regional Airport Authority, Mississippi

Checked November 18, 2026 at 7:22 PM UTC · Check ID d8a393e6-12c0-4e7d-b62c-87ee18afbdb8

**B**

**11** 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.



11 passed · 2 need attention · 3 missing

| Website | Email | DNS and domain |
|---|---|---|
| 6 of 8 | 3 of 5 | 2 of 3 |

### Not on a .gov domain

flypib.com 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. **Repair the SPF record** — HIGH RISK

   Receiving mail systems cannot tell the agency's real email from a forgery, so residents can receive fake notices in its name.

   **Fixed by: Your email or DNS provider**

2. **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**

3. **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**

4 **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**

5 **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 — 6 of 8 passed

#### HTTPS certificate — PASS

| | |
|---|---|
| Issued by | **WE1** |
| Issued to | **flypib.com** |
| Expires | **January 30, 2027 (72 days after this check)** |
| TLS version | **TLSv1.3** |

#### Redirect to HTTPS — PASS

| | |
|---|---|
| HTTPS available | **Yes** |
| Plain address redirects to HTTPS | **Yes** |

#### HSTS — PASS

| | |
|---|---|
| HSTS header | **Sent** |
| Max age | **31,536,000 seconds** |
| Includes subdomains | **Yes** |

#### 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 — PASS

| | |
|---|---|
| X-Frame-Options | **SAMEORIGIN** |

### File type protection — PASS

| | |
|---|---|
| X-Content-Type-Options | nosniff |

### 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 — 3 of 5 passed

### SPF — NEEDS ATTENTION

| | |
|---|---|
| Record | `v=spf1 include:zohomail.com ~all` |
| Ending | Soft fail (~all) |

**What this means:** Receiving mail systems cannot tell the agency's real email from a forgery, so residents can receive fake notices in its name.

**How to fix:** Publish one TXT record that lists every service sending mail for the domain and ends in -all. (Your email or DNS provider)

### DKIM — PASS

| | |
|---|---|
| Selectors found | zoho |

### DMARC — PASS

| | |
|---|---|
| Policy | quarantine |
| Reports sent to | da20b232edb1407493f0a970e69ffccc@dmarc-reports.cloudflare.net |
| Record | `v=DMARC1; p=quarantine; sp=quarantine; rua=mailto:da20b232edb1407493f0a970e69ffccc@dmarc-reports.cloudflare.net,mailto:35a8e406d060.a@dmarcinput.com; ruf=mailto:35a8e406d060.f@dmarcinput.com; fo=1` |

### MTA-STS — NEEDS ATTENTION

| | |
|---|---|
| DNS record | Found |
| Policy file | Found |
| Mode | testing |
| 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:35a8e406d060.m@dmarcinput.com` |

## 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 | Yes |

**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.

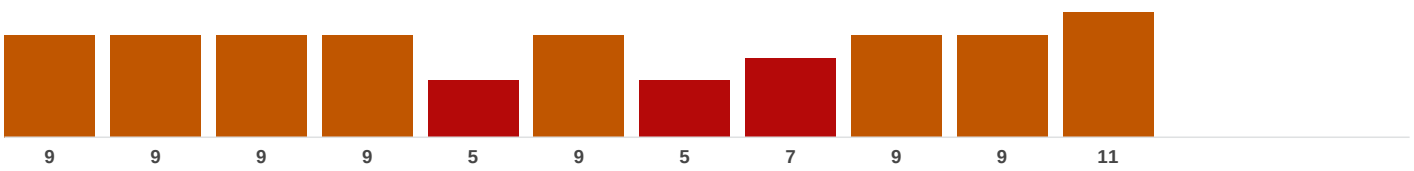
### Hosting and platform

Informational, not scored

| | |
|---|---|
| Website server | 104.21.4.12 |
| Mail server | mx.zoho.com |
| Website server reputation | Not on abuse lists |
| Mail server blocklists | Not listed |
| WordPress | Yes, version 7.1.5 |
| Email addresses published on the site | 0 |
| Broken links found | 2 |
| Referrer policy header | strict-origin-when-cross-origin |

## 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 5 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/flypib--com?check=d8a393e6-12c0-4e7d-b62c-87ee18afbdb8

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.