YesGov

GOVERNMENT DOMAIN SECURITY REPORT

# onawaymi.com

City of Onaway, Michigan · Population 912

Checked August 25, 2026 at 11:44 AM UTC · Check ID 63f4e74b-e834-42b2-b18e-5c351601d60e

**B-**

**10** 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.



10 passed · 6 missing

| Website | Email | DNS and domain |
|---|---|---|
| 4 of 8 | 3 of 5 | 3 of 3 |

### Not on a .gov domain

onawaymi.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. **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**

2. **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**

3. **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**

4 **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**

5 **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**

6 **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 — 4 of 8 passed

### HTTPS certificate — PASS

| | |
|---|---|
| Issued by | **WE1** |
| Issued to | **onawaymi.com** |
| Expires | **November 8, 2026 (74 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 — 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 — 3 of 5 passed

### SPF — PASS

| | |
|---|---|
| Record | `v=spf1 -all` |
| Ending | Strict (-all) |

### DKIM — PASS

| | |
|---|---|
| Selectors found | selector1, selector2, google, default, s1, s2, dkim, mail, smtp, mx, k1, k2, selector, mail1, mail2, smtp1, smtp2, dkim1, dkim2, mg, amazonses, ses, sg, sendgrid, mandrill, mailchimp, pm, postmark, sp, sparkpost, zoho, protonmail, outlook, office365, o365, hubspot, klaviyo, brevo, sendinblue, relay, gateway, outbound, inbound, bounce, newsletter, marketing, alerts, notify, system, admin, e911, hostingcp |

### DMARC — PASS

| | |
|---|---|
| Policy | reject |
| Reports sent to | 7f3c049ebedd4996ab4aeb1515f0cb3e@dmarc-reports.cloudflare.net |
| Record | `v=DMARC1; p=reject; sp=reject; adkim=s; aspf=s; rua=mailto:7f3c049ebedd4996ab4aeb1515f0cb3e@dmarc-reports.cloudflare.net` |

### 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 — 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:c633, 2606:4700:3036::6815:346f |
| 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.

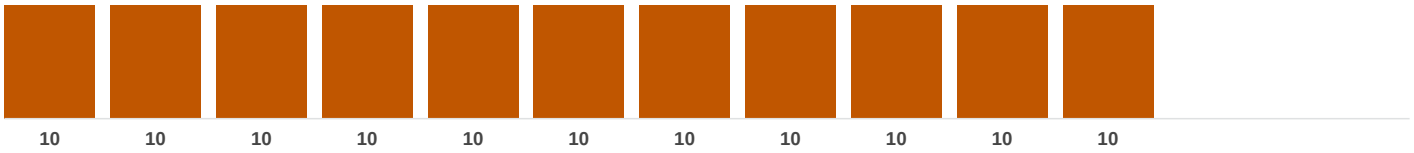
## Hosting and platform

Informational, not scored

| | |
|---|---|
| Website server | **172.67.198.51** |
| Mail server | **None found** |
| Website server reputation | **Not on abuse lists** |
| WordPress | **Not detected** |
| Email addresses published on the site | **0** |
| Broken links found | **1** |
| 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 6 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/onawaymi--com?check=63f4e74b-e834-42b2-b18e-5c351601d60e

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.