YesGov

GOVERNMENT DOMAIN SECURITY REPORT

on5g.com

Checked June 30, 2026 at 12:52 AM UTC · Check ID 1a17c319-59ac-4e29-8a38-ff9e7b8dc401

B+

12 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.



12 passed · 4 missing

Website	Email	DNS and domain
8 of 8	3 of 5	1 of 3

Not on a .gov domain

on5g.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. **Add a DMARC policy** — HIGH RISK
   Nothing tells receiving servers to reject mail that falsely uses this domain, so fake bills and payment requests in the agency's name are delivered.
   Fixed by: Your email or DNS provider

2. **Turn on DNSSEC** — HIGH RISK
   DNS answers are not signed. A forged answer can send residents to a fake payment page, or redirect the agency's email, with no visible sign.
   Fixed by: Your DNS host and domain registrar

3. **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

4 **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 8 of 8 passed

HTTPS certificate PASS

Issued by	**YesGov Managed**
Issued to	**on5g.com**
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 PASS

CAA record	**Found**
Authorities named	**Not captured in this scan**

Framing protection PASS

X-Frame-Options	**DENY**

File type protection PASS

X-Content-Type-Options	**nosniff**

Security contact (security.txt) PASS

/.well-known/security.txt	**Found**

Email 3 of 5 passed

SPF PASS

Record	`v=spf1 a:on5g.com mx:on5g.com include:spf.junkemailfilter.com include:_spf.smtp.com -all`
Ending	Strict (-all)

DKIM PASS

Selectors found	hostingcp

DMARC MISSING

DMARC record	Not found

What this means: Nothing tells receiving servers to reject mail that falsely uses this domain, so fake bills and payment requests in the agency's name are delivered.

How to fix: Publish a TXT record at _dmarc with p=quarantine or p=reject and an address to receive reports. (Your email or DNS provider)

MTA-STS PASS

DNS record	Found
Policy file	Found
Mode	enforce
Enforced	Yes

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 1 of 3 passed

DNSSEC MISSING

Zone signed	No
Result	No DNSSEC records found. DNSSEC may not be enabled for this domain.

What this means: DNS answers are not signed. A forged answer can send residents to a fake payment page, or redirect the agency's email, with no visible sign.

How to fix: Turn on DNSSEC signing at the DNS host, then add the DS record at the registrar. (Your DNS host and domain registrar)

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.

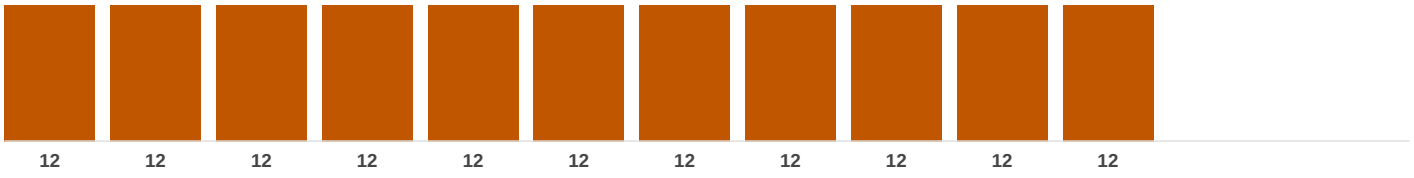
Hosting and platform

Informational, not scored

Website server	**23.145.20.51**
Mail server	**mail.on5g.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	**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 4 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/on5g--com?check=1a17c319-59ac-4e29-8a38-ff9e7b8dc401

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.