PERIMETRY RESEARCH

Security barometer of the UK State's domains

How well does the UK State protect its websites and e-mail? Passive measurements of the domains of GOV.UK, the departments, agencies, public bodies and devolved governments in open lists, compared with the French State.

November 2026 edition

236
domains with a site of their own, graded

74.6%
enforce DMARC (quarantine or reject)

30.1%
get an A or a B

Perimetry Cloud
perimetry.cloud · Published 14 November 2026

About this report

Perimetry Research publishes studies of how well organisations protect their websites and e-mail, measured with the same passive checks as Perimetry Cloud. This edition covers the 497 domains of the UK's central government in the Cabinet Office's list of .gov.uk domain names and the GOV.UK organisations; 463 are active, and the 236 with a site of their own are graded. It names only the domains that do well; every other figure is an aggregate, and the serious issues are reported to the NCSC before publication.

Contents

01 Executive summary 3

02 Key findings 4

03 Grades 5

04 Check by check 6

05 By category 8

06 Domains without a site of their own 9

07 Compared with the French State and our other studies 10

08 The domains that get it right 11

09 Serious issues 12

10 Recommendations 13

11 Methodology 14

12 About Perimetry 16

01

Executive summary

236
domains with a site of their own, graded

54
average score out of 100

74.6%
enforce DMARC (quarantine or reject)

30.1%
get an A or a B

Average score of the 236 graded domains: 54 out of 100; median 56.

1. 84.3% of the graded domains publish a DMARC policy and 74.6% enforce it (the French State: 43.3%).
2. Websites: 67.4% have a valid certificate, 75% send visitors to HTTPS, 42.1% use HSTS for six months or more.
3. 3.8% of the graded domains are signed with DNSSEC (the French State: 3.8%).
4. 227 active domains have no site of their own; 33.9% of them do not enforce DMARC.
5. On the same nine checks, the UK State averages 54 out of 100, the French State 46.

02

Key findings

The State's own indicators

25.5% of the active domains are outside .gov.uk.

0.2% of the listed domains are no longer in DNS.

84.3% of the graded domains publish a DMARC policy and 74.6% enforce it (the French State: 43.3%).

Websites: 67.4% have a valid certificate, 75% send visitors to HTTPS, 42.1% use HSTS for six months or more.

3.8% of the graded domains are signed with DNSSEC (the French State: 3.8%).

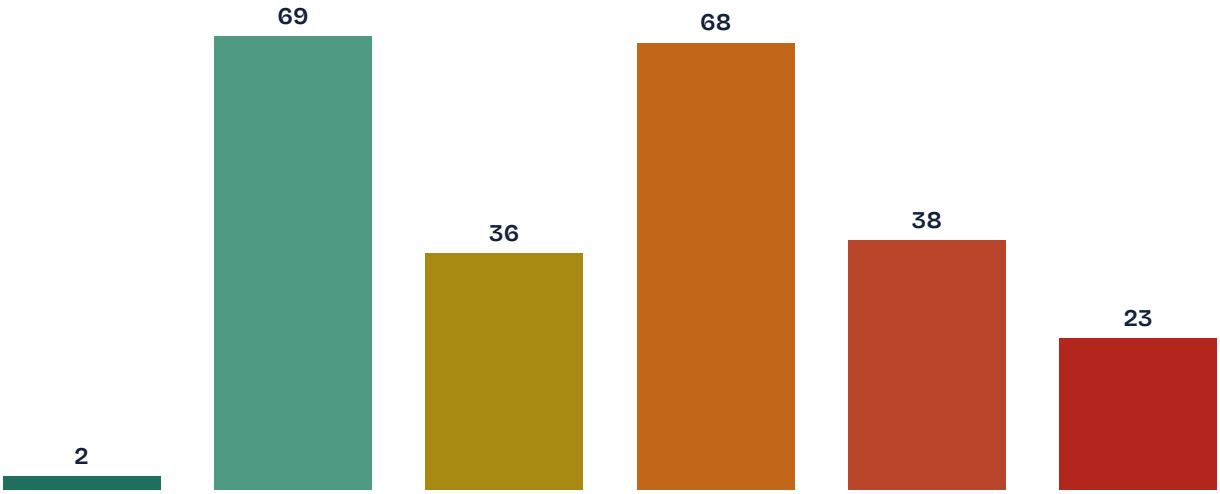
227 active domains have no site of their own; 33.9% of them do not enforce DMARC.

On the same nine checks, the UK State averages 54 out of 100, the French State 46.

03

Grades

Each domain with a site of its own gets a score: the share of the nine checks that it passes, among those that apply to it (the score of our other studies, without the check on the contact address, which the lists do not give). Grades: A from 90, B from 75, C from 60, D from 40, E from 20, F below.

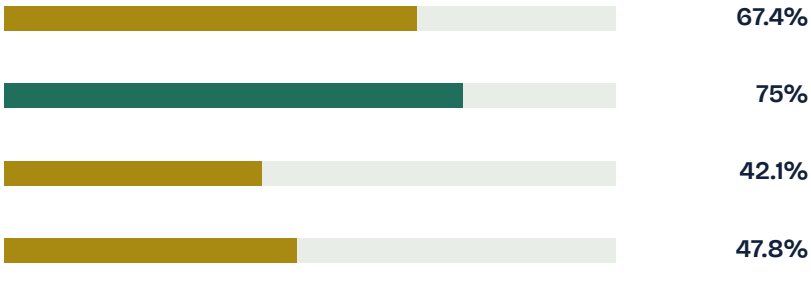


04

Check by check

Share of the graded domains that pass each check, among those it applies to.

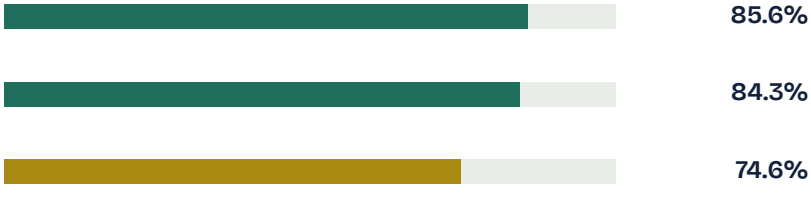
Website



DNS



E-mail



The nine checks	
Website · Valid HTTPS certificate	The site answers over HTTPS with a certificate that is in date, issued for its name, and trusted by browsers.
Website · HTTP sends visitors to HTTPS	Someone who types the address lands on the encrypted site, not on a page anyone on the network can read or alter.
Website · HSTS for six months or more	Browsers remember to use HTTPS only, so the first unencrypted request cannot be hijacked.
Website · Basic protective headers	X-Content-Type-Options: nosniff, and protection against being framed by another site (X-Frame-Options or CSP frame-ancestors).
DNS · DNSSEC	Answers about the domain are signed, so a resolver cannot be fed false addresses for the administration's site or mail.
DNS · CAA record	The domain names the certificate authorities allowed to issue certificates for it.
E-mail · Strict SPF	The domain lists the servers allowed to send its mail and asks receivers to reject or flag the others (-all or ~all).

The nine checks	
E-mail · DMARC record	The domain publishes a DMARC policy, the standard that ties SPF and DKIM to the visible sender.
E-mail · DMARC enforced	The policy is quarantine or reject: messages forged in the administration's name, to citizens for example, go to spam or are refused, not delivered.

05

By category

The GOV.UK organisations' own classification. Categories with fewer than ten graded domains show no figures.

Group	Graded	Average	A or B	DMARC enforced	Median
GOV.UK	1	·	·	·	·
Ministerial departments	61	36	6.6%	70.5%	33
Non-ministerial departments	15	54	46.7%	73.3%	–
Executive agencies	22	52	27.3%	77.3%	–
Public bodies (non-departmental)	116	65	42.2%	83.6%	67
Courts and tribunals	2	·	·	·	·
Devolved governments	12	40	25%	33.3%	–
Other central bodies	7	·	·	·	·

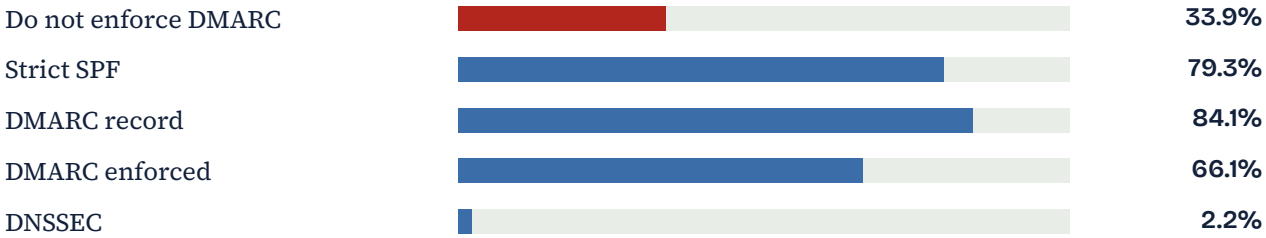
Average



06

Domains without a site of their own

227 active domains have no site of their own: 129 send visitors to another site, 98 are used for mail only. They can still be used to forge e-mail in the government's name, and are judged on DNS and mail only.



Average score on DNS and mail only: 47 out of 100.

07

Compared with the French State and our other studies

The same checks in our studies of the French State, communes, local authorities, higher education and .fr domains (latest editions): share of the graded domains that pass each one. The communes and local authorities count ten checks, the others nine.

	UK State	French State	Communes	Local authorities	Higher education	.fr domains
Average score	54	46	47	60	64	32
Valid HTTPS certificate	67.4%	63.8%	93.4%	98.7%	100%	59.1%
HTTP sends visitors to HTTPS	75%	77.3%	86.4%	90.9%	95.2%	53.4%
HSTS for six months or more	42.1%	33.3%	28.3%	38.8%	46.1%	17.3%
Basic protective headers	47.8%	51.9%	26.1%	40.7%	57.5%	14.1%
DNSSEC	3.8%	3.8%	22.1%	25.9%	12.7%	25.9%
CAA record	4.7%	18.5%	2.8%	2.6%	41%	1.2%
Strict SPF	85.6%	56.2%	85.9%	97.1%	93%	71.6%
DMARC record	84.3%	56.7%	45.2%	77.8%	86.9%	38.6%
DMARC enforced	74.6%	43.3%	19.2%	32.8%	45.4%	11.7%

08

The domains that get it right

2 domains pass every one of the nine checks and have no serious issue.

Domain	Category
officeforstudents.org.uk	Public bodies (non-departmental)
thenational.academy	Public bodies (non-departmental)

09

Serious issues

5 domains have a serious issue that could be used against them. They are not named in this report or anywhere else: they are reported to the NCSC before publication.



10

Recommendations

1 **Enforce DMARC on every domain, those without a site included**
A domain that only redirects to GOV.UK, or only sends mail, can be used to forge e-mail in the government's name. Every domain that sends no mail should publish an SPF record that allows nothing and a DMARC policy of reject.

2 **Turn on HSTS everywhere**
GOV.UK does; many bodies' own websites do not. HSTS makes browsers remember to use HTTPS only.

3 **Sign the domains with DNSSEC**
The .gov.uk registry supports it; few domains use it.

4 **Retire the domains no longer used**
Listed domains with neither a site nor mail should publish a policy that refuses mail, or leave the list.

5 **Watch it over time**
Certificates expire, providers change, records get lost in a migration. A regular check catches it before citizens do.

11

Methodology

Passive checks only

We read what any visitor or mail server can see: public DNS records, the domain registration (RDAP), the TLS certificate, one request for the home page over HTTP (its redirect is read, not followed), and the home page over HTTPS (following its redirects, as a browser would). Nothing else on the site is requested. When a domain publishes an MTA-STS policy, its policy file is read too, as mail servers do.

No port scanning, no subdomain discovery, no login attempts, no forms, no testing for vulnerabilities. The robot is slow on purpose and spreads its requests over several hours.

The robot

It identifies itself as PerimetryResearch/1.0 (+https://perimetry.cloud/research/methodology/). If you run a site it visited and would rather it did not, write to hello@perimetry.cloud and we will leave the domain out of the next editions.

The study of the UK State's domains

Population: the domains of the UK's central government in open lists under the Open Government Licence v3.0. GOV.UK itself, the single website of the ministerial departments and of most of their bodies. The domains of the Cabinet Office's list of .gov.uk domain names registered for a central government organisation: the latest editions of the list give the domain names only, so whom a domain is registered for is read in the edition of 30 March 2023, the last to say it, matched by name to the organisations of GOV.UK, and the domain is kept only if it is still in the latest edition (31 March 2026). And the websites of the GOV.UK organisations that keep one of their own (exempt from GOV.UK). Local government (councils, parish and town councils), the police and fire services are left out, as the French study leaves out communes and local authorities; so are public corporations (the BBC, Channel 4…) and the bodies GOV.UK classes as "other" (the Bank of England…).

Categories: the GOV.UK organisations' own classification (ministerial and non-ministerial departments, executive agencies, non-departmental public bodies, courts and tribunals, devolved governments, other central bodies). A domain registered after March 2023, or for a name that differs from the organisation's on GOV.UK, cannot be classified and is not in the study: the list is complete for the bodies' own websites, not for every .gov.uk domain of central government.

Everything else follows the study of the French State: inactive domains counted and left out, the main figures on the domains with a site of their own, the domains without one shown apart, nine checks, three that apply needed to be graded, groups of ten graded domains or more, only the domains that pass all nine checks named. The serious issues are reported to the NCSC before publication; the study gives their number only.

Good performers only

We name the communes that do well (the honour roll and the best of each size band), never the ones that do badly, and never a commune with a serious issue, whatever its score. Everything else is published as aggregates: by size of commune and by département, where a département with fewer than ten graded communes shows no figures, so that none of them can be singled out.

Website platforms are graded on a sample of up to five communes' sites there: a check counts as passed when most of the sample passes it.

Serious issues are reported privately

Some findings could be used against a commune right away: a domain listed in the official directory that no longer exists (anyone could register it), a registration the registry is deleting, an expired certificate, an SPF record that lets anyone send mail in its name. These are never published. We tell the commune first, quietly, and count them in the study without naming anyone.

Limits

Each edition is a snapshot taken over a few hours. The directory can be out of date or wrong; we use it as published. DKIM keys are looked for on common selectors only, so they are not graded. A site behind a protection service may answer differently to a robot than to a visitor. Mail servers are not tested (STARTTLS needs port 25, which the study's infrastructure cannot reach).

12

About Perimetry

Perimetry is an open source tool that audits the outside of a domain the way anyone on the internet sees it: e-mail authentication, DNS, certificates, mail servers, websites. Perimetry Cloud is its hosted version, with continuous monitoring, alerts and reports, for organisations and the agencies that look after them.

Cite as: Perimetry Research, Security barometer of the UK State's domains, November 2026. https://perimetry.cloud/research/uk-government/

You may reuse the figures of this report with a link to the study. Contains public sector information licensed under the Open Government Licence v3.0.

Contact: hello@perimetry.cloud

`https://perimetry.cloud/research/uk-government/`