PERIMETRY RESEARCH

Security barometer of the French State's domains

How well does the French State protect its websites and e-mail? Passive measurements of the domains of prefectures, ministries, académies, embassies and government sites in two open lists, compared with our other studies.

November 2026 edition

660
domains with a site of their own, graded

43.3%
enforce DMARC (quarantine or reject)

13%
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 1,440 domains of the State in the DINUM's list of public bodies' domain names and in the list of sites of the observatory of the State's digital ecosystem; 1,069 are active, and the 660 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 were reported to the CERT-FR of the ANSSI before publication.

Contents

01 Executive summary 3

02 Key findings 4

03 Grades 5

04 Check by check 6

05 By category 8

06 By kind of site 9

07 Domains without a site of their own 10

08 Compared with the other studies 11

09 The domains that get it right 12

10 Serious issues 13

11 Recommendations 14

12 Methodology 15

13 About Perimetry 17

01

Executive summary

660
domains with a site of their own, graded

46
average score out of 100

43.3%
enforce DMARC (quarantine or reject)

13%
get an A or a B

Average score of the 660 graded domains: 46 out of 100; median 44.

1. 56.7% of the graded domains publish a DMARC policy and 43.3% enforce it.
2. Websites: 63.8% have a valid certificate, 77.3% send visitors to HTTPS, 33.3% use HSTS for six months or more.
3. DNSSEC is rare: 3.8% of the graded domains are signed, against 22.1% for the communes.
4. 409 active domains have no site of their own; 63.3% of them do not enforce DMARC.
5. 18.5% of the State's active domains are outside .gouv.fr.

02

Key findings

The State's own indicators

18.5% of the active domains are outside .gouv.fr, the extension reserved for the State.

0.9% of the listed domains are no longer in DNS.

56.7% of the graded domains publish a DMARC policy and 43.3% enforce it.

Websites: 63.8% have a valid certificate, 77.3% send visitors to HTTPS, 33.3% use HSTS for six months or more.

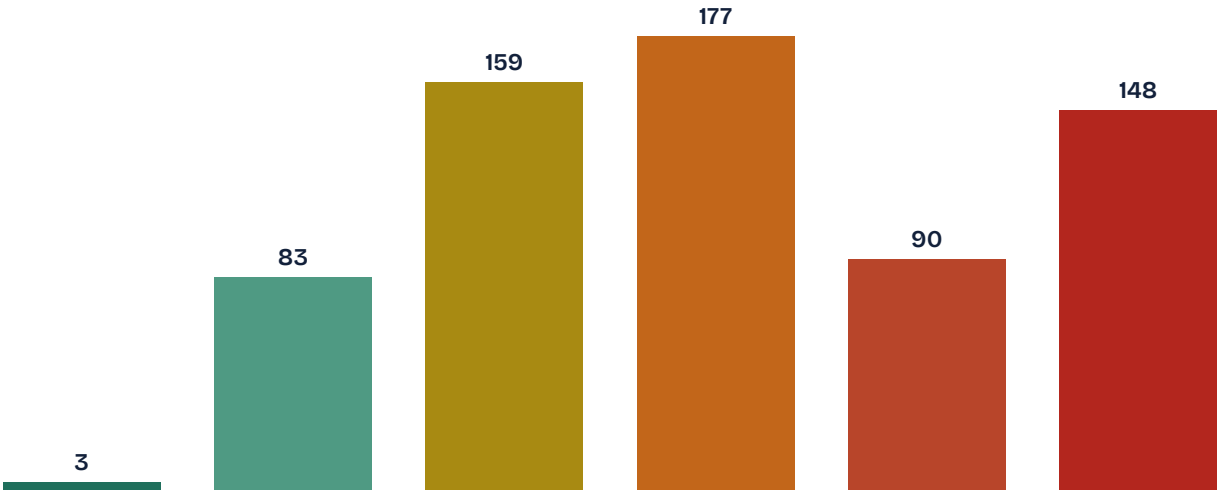
DNSSEC is rare: 3.8% of the graded domains are signed, against 22.1% for the communes.

409 active domains have no site of their own; 63.3% of them do not enforce DMARC.

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.

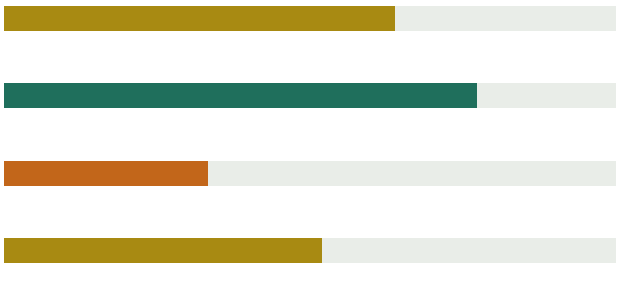


04

Check by check

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

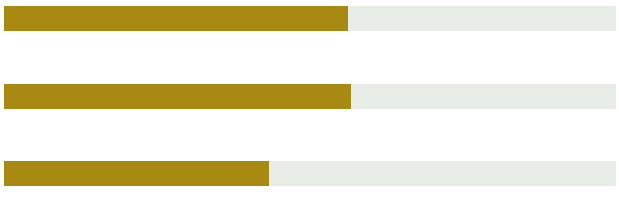
Website



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.

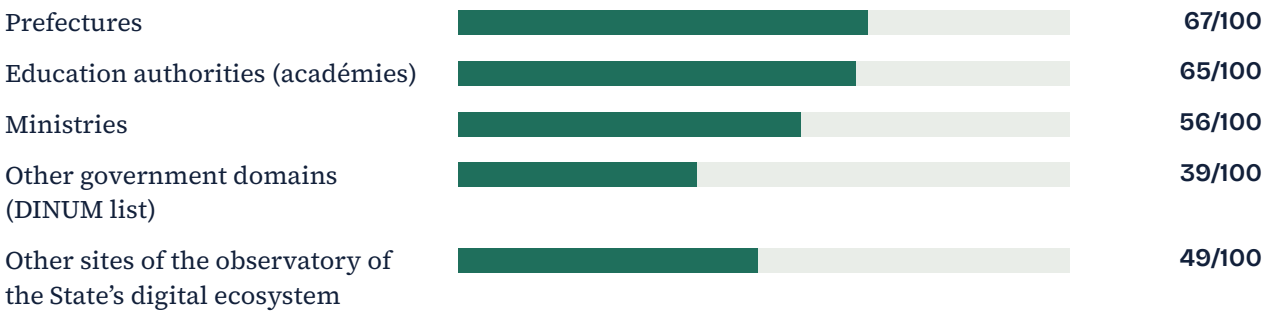
05

By category

Categories with fewer than ten graded domains show no figures. Most embassy domains send visitors to a site on another domain: they are counted among the domains without a site of their own.

Group	Graded	Average	A or B	DMARC enforced	Median
Prefectures	94	67	0%	100%	71
Education authorities (académies)	34	65	29.4%	32.4%	67
Embassies	2	·	·	·	·
Ministries	14	56	14.3%	14.3%	–
Health agencies	2	·	·	·	·
Other government domains (DINUM list)	465	39	14.4%	36.1%	44
Other sites of the observatory of the State's digital ecosystem	49	49	12.2%	18.4%	44

Average



06

By kind of site

The observatory's kinds of site, for the domains it lists.

Group	Graded	Average	A or B	DMARC enforced	Median
Institutional sites	175	65	13.1%	74.9%	71
Online procedures	21	65	52.4%	57.1%	–
Thematic sites	51	53	17.6%	31.4%	56
Other (open data, recruitment, events…)	34	56	23.5%	29.4%	56

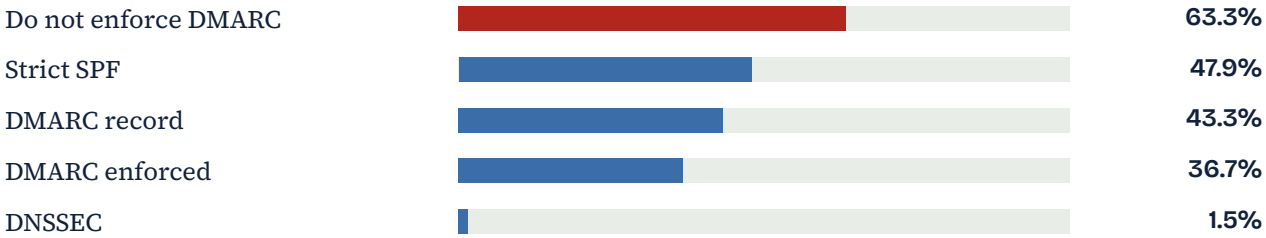
Average



07

Domains without a site of their own

409 active domains have no site of their own: 159 send visitors to another site, 250 are used for mail only. They can still be used to forge e-mail in the State's name, and are judged on DNS and mail only.



Average score on DNS and mail only: 28 out of 100.

08

Compared with the other studies

The same checks in our studies of the 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.

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

09

The domains that get it right

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

Domain	Category
douane.gouv.fr	Other government domains (DINUM list)
info.gouv.fr	Other government domains (DINUM list)
secnumacademie.gouv.fr	Other government domains (DINUM list)

10

Serious issues

78 domains have a serious issue that could be used against them. They are not named in this report or anywhere else: they were reported to the CERT-FR of the ANSSI before publication.



11

Recommendations

1 Enforce DMARC on every domain, those without a site included

A domain that only redirects or only sends mail can be used to forge e-mail in the State'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

Most sites already send visitors to HTTPS; HSTS makes browsers remember it, so the first request cannot be hijacked.

3 Sign the domains with DNSSEC

Under 4% of the State's graded domains are signed. The registry of .gouv.fr and most registrars support it.

4 Retire the domains no longer used

Hundreds of listed domains have neither a site nor mail. Kept registered, they should at least publish a policy that refuses mail; given up, they leave the lists.

5 Watch it over time

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

12

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 French State's domains

Population: the domains of the State in two open lists, both under the Licence Ouverte 2.0. The first is the DINUM's list of the domain names of public bodies (gitlab.adullact.net), its State types only: Gouvernement, Préfecture, Ministère, Académie, Ambassade and Santé (communes, local authorities, universities and hospitals have studies of their own). The second is the list of sites of the observatory of the State's digital ecosystem published by the Service d'information du Gouvernement (data.gouv.fr, file "audience-liste-sites"), without the sites it marks as parked. Each address is brought back to its registrable domain (interieur.gouv.fr is one domain); a domain in several groups is counted once, in the first of: prefectures, académies, embassies, ministries, health, other government domains, the observatory's other sites. The November 2026 edition counts 1,440 domains.

A domain is inactive, counted and left out, when it does not exist in DNS or has neither a site in use nor a mail server: many are former campaign or former body domains still listed.

The grades, the categories and the kinds of site are those of the domains with a site of their own. The active domains without one (a site that sends visitors to another domain, or a domain used for mail only) can only be judged on their DNS and mail: they are shown apart, as what they are, domains in whose name e-mail can be forged unless DMARC is enforced. Most embassy domains (ambafrance-xx.org) send visitors to a site on another domain: they are counted among them, so the embassies have too few graded domains to show figures.

The checks, score and grades of the communes study, without the check on the contact address, which the lists do not give: nine checks, as in the studies of higher education and of .fr domains. A domain needs three checks that apply to be graded; a group shows no figures below ten graded domains.

The honour roll names the domains that pass all nine checks and have no serious issue; no other domain is named. The serious issues (an expired certificate, DNS answers that fail, a listed domain anyone could register…) were reported to the CERT-FR of the ANSSI 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).

13

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 French State's domains, November 2026. https://perimetry.cloud/research/french-state/

You may reuse the figures of this report with a link to the study. The DINUM's list and the observatory's list remain under the Licence Ouverte 2.0.

Contact: hello@perimetry.cloud

`https://perimetry.cloud/research/french-state/`