

The CVE Panopticon

What happens when the prisoners set the standards?

The CVE Board is less transparent than my HOA.

I've said that in public.

Then I read all 116.

Discount me:

I'm a CVE data nerd and forecaster, and my employer runs on this catalogue.

549 CNAs publish every CVE record, under rules this Board approves.

CNA:

CVE Numbering Authority.

Rules v4.2.0, approved 20 August 2026.

MITRE runs the catalogue as Secretariat, under CISA.

This isn't the talk I promised.

The abstract promised Standard Scarcity:

80.8% of CVE records since 2023 name no fixed version.

The rule says SHOULD.

I'll bring you back to that 80.8% before I'm done.

What the Board decides.

It approves the CNA Operational Rules, decides who's a CNA, sets the record format and the dispute policy.

24 seats, every two weeks, minuted by a Secretariat of programme staff.

19 of 24 seats are held by employees of CNAs.

Those are the organisations the rules govern, and you'd want disclosure run by people who do it.

4 of the 24 are not ordinary voting seats: three liaison, one MITRE at-large

16 of 20 ordinary voting seats at CNA employers, counting only the 20 ordinary seats

ANSI: a standards process “shall not be dominated by any single interest category”, and the developer must record every voting member's category.

Nobody makes this Board record who voted at all.

Three incomplete archives. No two agree.

Two archives of the Board’s public list, and the meeting-summary PDFs.
Decisional votes go to a second Board list with no public archive.

SOURCE	WHAT IT IS	COVERAGE
marc.info	Independent archive of the Board list, 2022 onward.	sees 99 of 116
mail-archive.com	The archive the CVE Program links to.	sees 89 of 116
Meeting summary PDFs	Published to cve.mitre.org, dead on the live site, recovered from the Internet Archive.	sees 76 of 116

Only 50 of 116 meetings appear in all three. 18 appear in exactly one.

Pick any one source and you lose between 15 and 34 percent of the record.

What I pulled, and where from.

1,208 member-meeting attendance records, across 53 meetings

455 sentences mentioning a vote, motion, quorum or abstention, classified by regex and all published

21 tallied vote outcomes, at least, across 13 meetings

No leaks, no insider access, no private documents.

All of it is what the Board chose to publish, so this is the dataset that flatters them most.

Attendance ships per person, under the names the Board published in its own rosters.

CNA Operational Rules, section 2.1.4.

“Changes **MUST** be considered, decided, and documented in a transparent process.”

The Board wrote it, approved it, and is bound by it.

CNA OPERATIONAL RULES 1.4

MUST Mandatory **SHOULD** Recommended **MAY** Discretionary

Section 1.4 defines the terms, and **MUST** is the strongest one they had.

The charter adds three more promises.

CVE BOARD CHARTER V3.5	TEXT	STATUS
2.13.1 Snap votes	A snap vote is taken live on a Board call. “A required quorum is defined as one more than half the membership of the Board must be on the call.” Unanimous consent required to pass.	Discussed six times. The count moves to a private list and is not published.
2.13.3 Proxy voting	“The Secretariat is responsible for documenting the name of an absent Board voting member and the designated proxy voter on a per vote basis.”	No such record is public.
2.8 Removal	A member may be removed for “lack of participation.”	Used at least once, in 2018. The Board’s own record does not show it.

Section 2.14 adds a fourth: policy changes must have “transparent change control mechanisms.”

Some of this is open, and I should say so.

PROVISION	WHAT IT SAYS	EFFECT
Charter 2.16	Working Groups are open by default, but only “if the charter does not restrict participation.”	Two of them, strategic planning and quality, state they are “not open to participation from the public at large.”
Charter 2.15.1	Executive Sessions cover nominations, member removals and departing member status. No notes by default.	A published, reasoned confidentiality rule.

Section 2.16 also says a recommendation nobody responds to counts as approved, so a whole class of decisions produces no vote at all.

My complaint sits between the two rows: the vote that turns a draft into a rule, and the attendance that says who was there to cast it.

How does the Board decide?

No vote in the record has a name on it.

0

votes in 116 published meetings record how any individual member voted.

55 of 116 meetings discuss a vote.

19 record an outcome.

13 give a vote count.

None record a name, 2021 to 2026.

Votes are counted. Out of how many?

Meeting	Tally as recorded	Out of	What was decided
2021-11-10	9 of 11	11 on call	Two-week soft launch
2022-01-19	10 of 13	13 on call	Summit date and time
2022-09-28	10 to 0	those in attendance	Soft Deploy start
2022-09-28	16 yes, 0 no	not stated	Record Dispute Policy
2024-04-03	12 of 12	12 in the meeting	Whether to hold a vote
2024-07-24	12 yes	not stated	CNA Rules 4.5.2.4 rewording

The 13 meetings that give a count hold at least 21 of them, because some meetings voted more than once. Only 11 say out of how many.

A vote is valid only with “at least a simple majority of the eligible Board members” (Charter 2.13.2). Without the “out of” number, nobody outside can check that.

63 meetings with no attendance published.

Published 2021-06 to 2022-08 · 24	Nothing published 2022-08-17 to 2025-04-16 · 63 meetings	Published 2025-04 to 2026-08 · 28
---	--	---

Two years and eight months, 2022 to 2025.

No published minute records the decision to stop, or the decision to resume.

Maybe a template lost a section, maybe the Board decided, and the published record can't tell you which.

The Board was publishing attendance as far back as 2018.

August 2022: the Board reviews its own absentees.

Every quotation is from the Board's published minutes.

I'm not claiming anyone did this on purpose.

2022-08-03 Action item: the Program Coordination Team “will reach out to Board members individually that have poor meeting attendance/program engagement.” **Last meeting with published attendance.**

2022-08-17 Open Discussion item, “**Board Member Attendance**”: “Five members with low attendance were contacted.” **First meeting with no attendance published.**

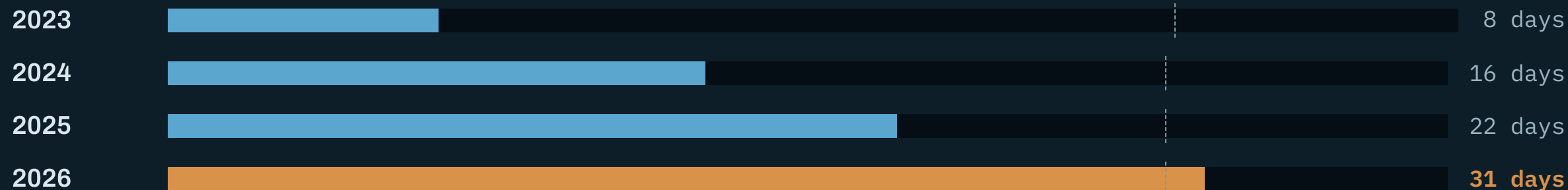
2022-09-28 Another said meetings are “too operationally or tactically focused to justify attendance.” **“Removal of inactive Board members”** goes on the future agenda.

2022-10-12 The review closes as complete: “Inactive members have responded; no further action is needed.” No removal vote is ever recorded.

next 63 meetings No attendance published. Meeting-summary PDFs keep coming, 50 of them, without the roster section.

Attendance stopped being published in the same fortnight the Board started contacting members about attendance.

Minutes are taking longer to publish.



Median days from meeting to published minutes, 2023 onward, where list coverage is near complete.

In 2026, 7 of 12 meetings took more than 30 days, the dashed line.

One clause changed after the rules were approved.

Apr to May 2024 CNA Rules 4.0 goes to a full Board vote on the mailing list. “The vote on new rules passed, voting technically stays open until May 9.” This is the process working.

2024-07-24 “SNAP VOTE: CVE Board votes 12 yes to change language in the second clause of 4.5.2.4.”

2024-08-07 “Releasing blog on Thursday, August 8th about the CNA rules 4.0 becoming official.” The amended text ships.

Charter 2.13.1 says snap votes “cannot be used for approving policy documentation initial approvals or subsequent updates.” No ratifying list vote appears in the fifteen days between.

They **do** track quorum. You just can't see it.

2022-09-28 “A Board quorum was not present.” They said so, then recorded the vote as 10-0 of those attending.

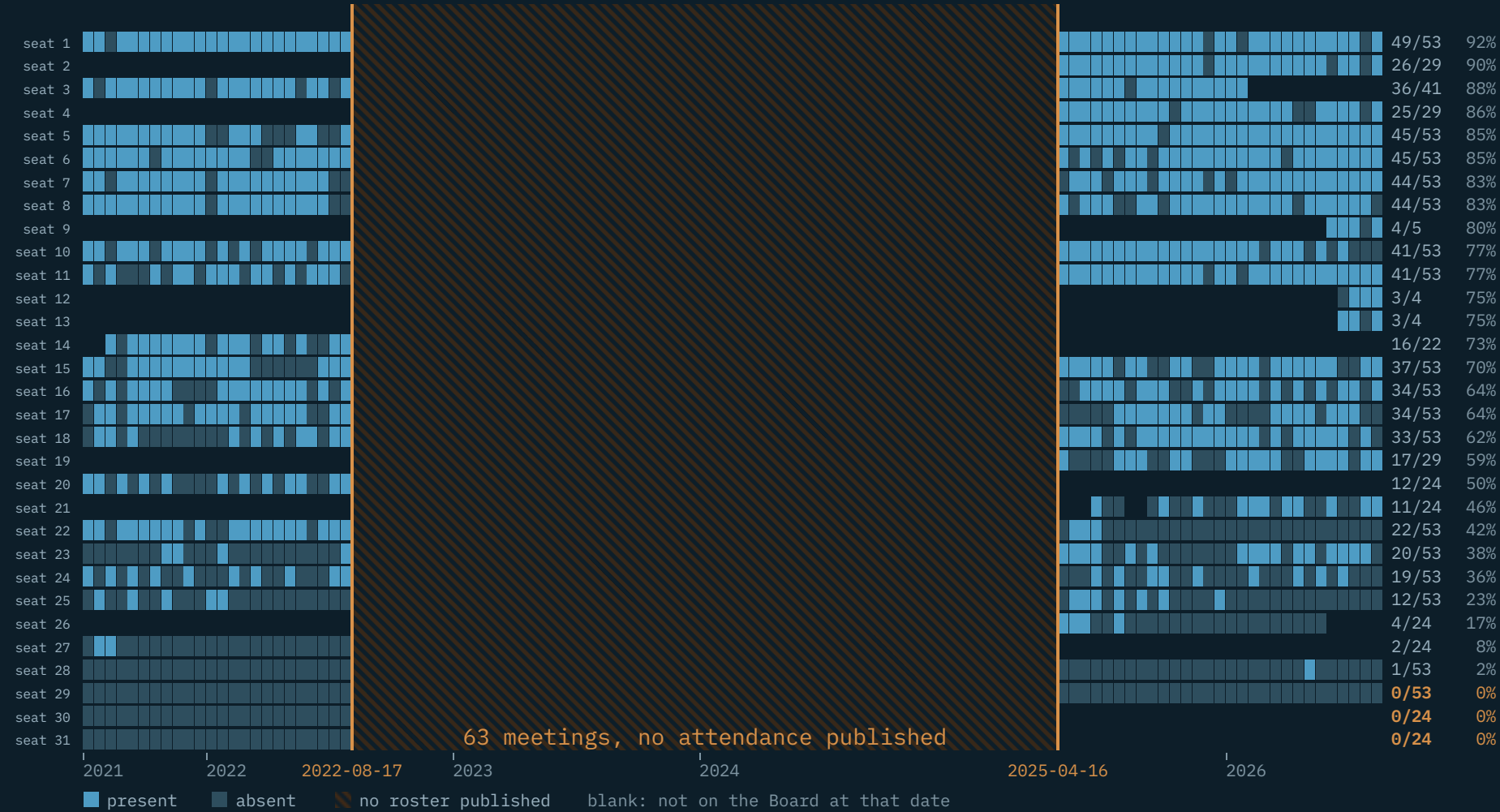
2023-01-04 “This was not a quorum, so an email will be sent to the Board private list asking members who could not attend to cast their vote.” Correct escalation.

2024-09-18 “Quorum of 11 members present voted unanimously to cancel the current vote.”

Six meetings discuss quorum, and the practice they describe is what the charter asks for.

Then the vote moves to the private Board list, where the count that makes it valid is never published.

Every member, every meeting.



31 people on the published rosters for 24 seats since June 2021, one of them programme staff. Fractions count only the 53 rostered meetings, the most generous reading available.

Charter 2.8 has been used. The record doesn't say so.

0 of 53

meetings attended by one sitting Board member across five years.

Two more seats are at zero over shorter tenures, and all three are still on the roster.

Turnout across 31 seats and 53 rostered meetings averages 56 percent, and the median seat is at 64.2. Before and after the blackout it reads 51.3 and 60.5, but 13 seats aren't in both eras.

For the 18 who are, it's 58.3 to 59.8.

Charter 2.8 lists “lack of participation” as grounds for removal and runs the whole process on the private Board list.

The only public account of a removal, from 2018, is the removed member's own post.

Participation also includes voting on that list, which isn't published either, so a seat at zero attendance may be voting every fortnight and nobody outside can tell.

Departures are recorded. Reasons aren't.

14 Emeritus, on cve.org

49 Other Past Contributors, on cve.org

1 Emeritus grant by snap vote, October 2024, shown on the page

Charter 2.15.1 keeps the deliberation in Executive Session, and that rule is published. Nothing says whether any of the 49 left by resignation, expiry or a 2.8 removal.

OWASP publishes every board member’s vote, by name.

Ashwini Siddhi	YES	Avi Douglen	YES
Diego Silva Martins	YES	Harold Blankenship	YES
Sam Stepanyan	YES	Steve Springett	YES
Ricardo Griffith	YES		

Results: Passes 7-0

OWASP Global Board, April 2025, verbatim, as published on every motion.
This one was unanimous, and the record would look the same if it hadn’t been.

Debian chose secrecy, in public.

Debian published names beside ballots until 2022.

A public General Resolution moved it to secret ballots.

The tally is still published, and the choice is on the record.

A California homeowners association owes its members more than a CNA gets.

A HOMEOWNER CAN

BECAUSE STATUTE SAYS SO

A CNA CANNOT

Attend the meeting

Civil Code 4925: members may attend open board meetings, on four days notice, with a published agenda.

Closed to the public.

Speak before the vote

Members may address the board on agenda items before it acts.

Comment happens in working groups, not at the vote.

In 2023 the Board would have cleared the California rule easily.
In 2026 it misses it more often than it makes it.

“They are volunteers, and this is a technical body.”

True, and the charter says so.

It also says voting “is a core responsibility,” that members must “participate by voting as often possible,” and that abstentions count toward participation.

A volunteer can miss a meeting, and the record of who missed it went unpublished for two years.

Three other volunteer technical bodies, and what each of them publishes:

OASIS ballot results

W3C formal objections

IETF consensus calls, on lists you can read now

“Nothing bad has happened.”

Maybe not.

You can't know that, and neither can I.

An institution whose decisions cannot be audited does not get credit for passing an audit it never allowed.

This is the Standard Scarcity talk, one level down.

the symptom 80.8 percent of CVE records since 2023 do not name a fixed version. In 2026 alone, 78.6 percent.

the cause CNA Rules 5.1.5: “SHOULD identify Fixed versions of Products.” Recommended, under their own definitions.

the lever Turning a SHOULD into a MUST requires a full Board vote under charter 2.14.

the problem That vote is unobservable. No roll-call vote ever, no denominator on the ones taken off the call, no attendance for 63 meetings.

You can't lobby a process you can't see, and that's why this talk comes before the other one.

None of this needs new infrastructure.

ASK	WHAT IT MEANS	COST
Publish the roll-call vote	Which member voted, and how. The vote is already called in the room.	A name beside each vote
Publish attendance	They published this for 53 meetings and the charter's private list exists for the rest.	Restore a section
State the denominator	Say "14 of 23 eligible" instead of "14 votes cast." Charter 2.13.2 makes eligible members the test of a valid vote, and nobody outside can check it today.	Six characters

The first row is the ask.

The other two apply the same change to what they already publish.

Publish the roll-call vote.

The count is already taken, and the charter names every proxy voter.

Executive Session stays closed, minuted as having happened.

Most of you work for a CNA and can ask.

The rule they wrote for themselves.

“Changes **MUST** be considered, decided, and documented in a transparent process.”

Rule 2.1.4, approved 20 August 2026.

Mandatory.

Sources and method

THE CORPUS

116 distinct CVE Board meetings, 2021-06-23 to 2026-08-19, merged and de-duplicated from three incomplete archives: the marc.info mirror of the Board list, the mail-archive.com copy that the CVE Program links to, and the meeting-summary PDFs that were published to cve.mitre.org and now survive only in the Internet Archive. No source is complete. Only 50 of 116 meetings appear in all three.

ATTENDANCE

Parsed from the checkbox rosters in the meeting-summary PDFs, 1,208 member-meeting records across 53 meetings. Nothing can be claimed about the other 63, and nothing here tries to. Published attendance goes back at least to the 22 August 2018 summary in cve.org's old Board list archive ([.../data/board/archives/2018-08/msg00026.html](http://data/board/archives/2018-08/msg00026.html)).

REMOVAL

The only public account of the 2018 removal is the removed member's own post of 31 August 2026 (jericho.blog/2026/08/31/how-much-lipstick-can-that-cve-pig-wear/). The Board published nothing.

VOTES

Every sentence mentioning a vote, motion, quorum or abstention was extracted by regex and published, so anyone can reclassify them. Tallied outcomes were swept from the same corpus with a rejection log.

CHECKING

102 claims re-derive from source on every build. 52 are derived: the expected value is a boolean, an empty counterexample set, or an exact quotation from a source document. 50 are asserted: the expected value is a number this pipeline emitted earlier. An asserted claim proves a number has not changed. It does not prove the number is right, and it is listed as asserted for that reason.

THE DATA

Published per person at github.com/jgamblin/Panopticon, under the names the Board published in its own rosters. The attendance grid on the slide uses seat numbers instead, as a presentation choice and not as anonymity: the named file is public, and the numbering is not meant to hide anyone. Rows run by attendance rate, and every row carries its present and eligible counts, so a seat measured over 4 meetings cannot pass for one measured over 53.

CAVEATS CARRIED INTO EVERY SLIDE

Attendance exists for 53 of 116 meetings. Two roster names are merged as one seat. One MITRE staff seat is not a voting seat. Minutes since 2025 disclose that drafts were generated by a meeting assistant. Correlation is never presented as intent.

Caveats, in full

ATTENDANCE

Rosters exist for 53 of 116 meetings. Nothing is claimed about the other 63, and every attendance rate counts only the meetings where that member was on a published roster. That is the most generous reading available, and it is the one used throughout.

31 people appear on the published rosters for 24 seats since 2021-06-23. Two roster names are merged as one seat. One seat is programme staff rather than a voting member. The turnout pair 51.3 and 60.5 compares two different Boards: 13 of the 31 seats are not in both eras, and for the 18 who are it is 58.3 to 59.8.

VOTES

21 tallies is a floor, not a count. The sweep is a regular expression over 116 documents with a published rejection log, and it found two rows in one evening that four review rounds had missed. Read every tally number as "at least".

THE NULL RESULT

The record-quality comparison rests on 11 Board-affiliated vendor CNAs against 160 other assigners publishing 50 or more records since 2023. $n=11$ is small. One real difference survives: median days to publish is 48 against 36.5, which points at slower, not worse.

INTERPRETATION

The blackout and the inactive-member review overlap in time. That is correlation and it is presented as correlation. No motive is alleged anywhere in this deck, and the likeliest explanation, a template that lost a section, is stated on the face.

Minutes since 2025 disclose that drafts were generated by a meeting assistant.