Complaint regarding BCP 79 violations

Daniel J. Bernstein, 2025-05-26

This is a complaint to the Internet Architecture Board (IAB) regarding recent violations of two provisions of BCP 79 (RFC 8179).

The two BCP 79 provisions at issue are identified below. The documents at issue are https://datatracker.ietf.org/doc/draft-ietf-lamps-kyber-certificates/ and https://datatracker.ietf.org/doc/draft-ietf-lamps-cms-kyber/. My understanding is that the documents are under current IESG consideration (first by an IESG member designated as the relevant "area director" and then by the full IESG), making it important for IAB to handle this complaint in a timely fashion.

IETF Administration LLC claims (https://www.ietf.org/blog/ietf-llc-statement-competition-law-issues/) that "IETF activities are conducted with extreme transparency, in public forums". The relevant public mailing list for the documents at issue is spasm@ietf.org. For transparency, please carry out all discussion of this matter on that list, including, but not limited to, any discussions of this matter among IAB members, IESG members, agents of IETF Administration LLC, etc.

Procedurally, I have three independent grounds for requesting IAB attention to this matter:

- BCP 39 (RFC 2850) states: "The IAB provides oversight of the process used to create Internet Standards [BCP 9]." This creates a general obligation upon IAB to monitor problems with that process.
- BCP 39 also states: "The IAB serves as an appeal board for complaints of improper execution of the standards process, with powers defined in [BCP 9]." BCP 9 (RFC 2026) creates a specific obligation upon IAB to "review the situation and attempt to resolve it" when a disagreement "is not resolved to the satisfaction of the parties at the IESG level"; that is the case for the specific action at hand.
- Standardization organizations are obliged by law to provide an appeals process *and* due process for all interested parties, among other obligations; see below. IETF's handling of this specific matter so far is not meeting these obligations.

The first two grounds by themselves leave IAB tremendous flexibility: BCP 39 does not specify concretely what "oversight" means, and BCP 9 says that IAB shall attempt to resolve disagreements "in a manner of its own choosing". But the fact that this flexibility exists is another due-process violation.

Three types of problems are numbered in the margins below: **F** for factual issues, **I** for violations of IETF policy, and **A** for violations of the requirements that antitrust law places upon standardization organizatons. Please make sure to specifically respond to each of these.

1 Criminal antitrust law

I'll begin by explaining what I said above about legal obligations. I'll focus on United States antitrust law here.

First point: **an agreement in restraint of interstate commerce is a felony.** Here's what the law says (source: https://uscode.house.gov/view.xhtml?req=(title:15%20section:1%20edition:prelim)):

> Every contract, combination in the form of trust or otherwise, or conspiracy, in restraint of trade or commerce among the several States, or with foreign nations, is declared to be illegal. Every person who shall make any contract or engage in any combination or conspiracy hereby declared to be illegal shall be deemed guilty of a felony, and, on conviction thereof, shall be punished by fine not exceeding $100,000,000 if a corporation, or, if any other person, $1,000,000, or by imprisonment not exceeding 10 years, or by both said punishments, in the discretion of the court.

Antitrust law is in the news mainly in the context of big corporations being forcibly restructured, but https://web.archive.org/web/20250424170656/https://www.ussc.gov/sites/default/files/pdf/about/commissioners/selected-articles/Howell_Review_of_Antitrust_Sentencing_Data.pdf shows that quite a few people have been sent to jail.

Second point: **the law makes an exception for standardization, but invoking the exception requires conduct to meet the law's definition of "standards development activity", and to be carried out by an organization meeting the law's definition of a "standards development organization"**. Here's the exception in the law (source: https://uscode.house.gov/view.xhtml?req=(title:15%20section:4302%20edition:prelim)):

> In any action under the antitrust laws, or under any State law similar to the antitrust laws, the conduct of-
>
> (1) any person in making or performing a contract to carry out a joint venture, or
>
> (2) a standards development organization while engaged in a standards development activity,
>
> shall not be deemed illegal per se; such conduct shall be judged on the basis of its reasonableness, taking into account all relevant factors affecting competition, including, but not limited to, effects on competition in properly defined, relevant research, development, product, process, and service markets.

Third point: **an organization is not a "standards development organization" under this law unless it meets the OMB A-119 criteria**. Here's the definition of "standards development organization" in the law (source: https://uscode.house.gov/view.xhtml?req=(title:15%20section:4301%20edition:prelim)):

> The term "standards development organization" means a domestic or international organization that plans, develops, establishes, or coordinates voluntary consensus standards using procedures that incorporate the attributes of openness, balance of interests, due process, an appeals process, and consensus in a manner consistent with the Office of Management and Budget Circular Number A–119, as revised February 10, 1998. The term "standards development organization" shall not, for purposes of this chapter, include the parties participating in the standards development organization.

Fourth point: **the OMB A-119 criteria place specific requirements upon consensus, along with requiring openness, due process, and more**. Here's the OMB A-119 definition of a voluntary consensus standards body (source: https://www.govinfo.gov/content/pkg/FR-1998-02-19/html/98-4177.htm):

> A voluntary consensus standards body is defined by the following attributes: (i) Openness. (ii) Balance of interest. (iii) Due process. (vi) An appeals process. (v) Consensus, which is defined as general agreement, but not necessarily unanimity, and includes a process for attempting to resolve objections by interested parties, as long as all comments have been fairly considered, each objector is advised of the disposition of his or her objection(s) and the reasons why, and the consensus body members are given an opportunity to change their votes after reviewing the comments.

Fifth point: **activity by a standards development organization is still not "standards development activity" under the law unless it has one of the standardization/conformity-assessment purposes specifically listed in the law *and* avoids the activities specfically excluded in the law**. Here's the definition of "standards development activity" in the law (source: https://uscode.house.gov/view.xhtml?req=(title:15%20section:4301%20edition:prelim)):

> The term "standards development activity" means any action taken by a standards development organization for the purpose of developing, promulgating, revising, amending, reissuing, interpreting, or otherwise maintaining a voluntary consensus standard, or using such standard in conformity assessment activities, including actions relating to the intellectual property policies of the standards development organization. . . . The term "standards development activity" excludes the following activities:

(1) Exchanging information among competitors relating to cost, sales, profitability, prices, marketing, or distribution of any product, process, or service that is not reasonably required for the purpose of developing or promulgating a voluntary consensus standard, or using such standard in conformity assessment activities.
(2) Entering into any agreement or engaging in any other conduct that would allocate a market with a competitor.
(3) Entering into any agreement or conspiracy that would set or restrain prices of any good or service.

To summarize: Relabeling an agreement to restrain commerce as “standardization” is not a get-out-of-jail-free card. The exception in antitrust law for standardization applies only under a series of restrictions, including the following. All actions must be for the purpose of standardization or conformity assessment, and must be taken only with consensus. A consensus declaration does not require unanimity, but it must be preceded by

- general agreement;
- fair consideration of each comment;
- a process of attempting to resolve each objection; and
- documentation—for any objection that was not resolved but that was instead overridden by general agreement—of why that objection was overridden.

As further protections, there must be openness, a balance of interests, an appeals process, and due process. When *all* of these requirements are met, the standardization activity is not “deemed illegal per se”, and a court will instead evaluate “reasonableness” as the dividing line between the activity and a felony.

2 The BCP 79 provisions at issue

The first BCP 79 provision at issue is the “no known IPR claims” requirement for “mandatory-to-implement security technology”:

> It has become common to have a mandatory-to-implement security technology in IETF technology specifications. This is to ensure that there will be at least one common security technology present in all implementations of such a specification that can be used in all cases. This does not limit the specification from including other security technologies, the use of which could be negotiated between implementations. An IETF consensus has developed that no mandatory-to-implement security technology can be specified in an IETF specification unless it has no known IPR claims against it or a royalty-free license is available to implementers of the specification. It is possible to specify such a technology in violation of this principle if there is a very good reason to do so and if that reason is documented and agreed to through IETF consensus. This limitation does not extend to other security technologies in the same specification if they are not listed as mandatory to implement.

The second BCP 79 provision at issue is the “change control” requirement:

> The IETF must have change control over the technology described in any Standards Track IETF Documents in order to fix problems that may be discovered or to produce other derivative works.
>
> In some cases, the developer of patented or otherwise controlled technology may decide to hand over to the IETF the right to evolve the technology (a.k.a., ‘‘change control’’). The implementation of an agreement between the IETF and the

> developer of the technology can be complex. (See [RFC1790] and [RFC2339] for examples.)
>
> Note that there is no inherent prohibition against a Standards Track IETF Document making a normative reference to proprietary technology. For example, a number of IETF standards support proprietary cryptographic transforms.

3 Kyber patent timeline

The factual background for the specific BCP 79 violations at issue, in short, is as follows. GAM (Gaborit and Aguilar Melchor), Ding (Jintai Ding), and Zhao (Yunlei Zhao) have patents that they say cover NIST's new ML-KEM standard (Kyber). NIST says it has signed patent licenses for the GAM (owned by CNRS) and Ding patents, but, in the Ding case, *only* for *exactly* the NIST-standardized version of ML-KEM, not for any modifications. There have been no comments from NIST regarding the Zhao patents.

In more detail, the timeline of events is as follows:

- 2021-08-20: NIST said (https://groups.google.com/a/list.nist.gov/g/pqc-forum/c/GO3Wj9VLOoM/m/Batpm9efAAAJ) that input to the NIST Post-Quantum Cryptography Standardization Project is due 2021-10-31.
- 2021-10-25: An internal NIST document (https://nist.pqcrypto.org/foia/index.html#20230105/KSN%20Document.docx) listed the following "IP issues" for Kyber: "CNRS patent, Jintai's?"
- 2022-03-02: An internal draft of the NIST selection report (https://nist.pqcrypto.org/foia/index.html#20240924/ERB%20readers%20for%20PQC%20report.pdf-attachment-draft%20PQC_3rd_Round_Report.pdf) said that NIST is standardizing Kyber; said that "ISARA, the French National Centre for Scientific Research (CNRS), and Dr. Jintai Ding" owned "patents that may have potentially impacted some of the lattice-based KEM algorithms"; and said that NIST "has reached agreements that will provide worldwide royalty-free and nondiscriminatory licenses for implementing the standard".
- 2022-04-19: NIST said (https://groups.google.com/a/list.nist.gov/g/pqc-forum/c/fvnhyQ25jUg/m/izNIg5BABwAJ) that "the delay is not due to technical considerations but is due to some legal and procedural steps that are taking more time than we anticipated".
- 2022-05-12: Yunlei Zhao (https://groups.google.com/a/list.nist.gov/g/pqc-forum/c/Fm4cDfsx65s/m/F63mixuWBAAJ) said that "Kyber is covered by our patents (not only the two patents mentioned in the KCL proposal, but also more patent afterforwards)", and said (https://groups.google.com/a/list.nist.gov/g/pqc-forum/c/Fm4cDfsx65s/m/7HJShM2dBAAJ) that the patents are for "credit (not for economic reasons)".
- 2022-07-04: NIST announced (https://web.archive.org/web/20220705160405/https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8413.pdf) standardization of Kyber; similar text to the 2022-03-02 draft.
- 2022-11-30: NIST said (https://groups.google.com/a/list.nist.gov/g/pqc-forum/c/4MBurXr58Rs/m/WX3u_lU_AQAJ) that licenses had been signed with CNRS (GAM patent) and Ding. NIST posted edited excerpts from the licenses: https://web.archive.org/web/20221130033932/https://csrc.nist.gov/csrc/media/Projects/post-quantum-cryptography/documents/selected-algos-2022/nist-pqc-license-summary-and-excerpts.pdf

There are two factual questions that have been raised and that don't seem to be answered by the available documents:

- Did NIST evaluate the Zhao patent claim regarding Kyber?
- Why didn't NIST post the complete signed licenses for the GAM and Ding patents?

Regarding the second question, there is a third-party claim (https://mailarchive.ietf.org/arch/msg/spasm/GKFhHfBeCgf8hQQvhUcyOJ6M-kI/) that NIST has released “all of the information about the licenses that it can”. This claim doesn’t seem to be substantiated.

4 How these drafts violate the provisions at issue

The notation in Figure 1 as follows: “con” means an argument that the draft is violating BCP 79; “pro” means an argument that the draft isn’t violating BCP 79; “fix” means a potential way forward.

Indenting B under A in the figure indicates that B is a supporting argument for A (if same pro/con) or a counterargument to A (if opposite pro/con) or a fix for A. Links are to mailing-list messages that have raised these arguments and counterarguments. The figure applies equally to both drafts.

In general, the easy way to see that the “pro” arguments in Figure 1 are flawed is to see that they prove too much: they would allow any draft to simply ignore these BCP 79 requirements.

Exception: there are two counterarguments that really are specific to the situation at hand, namely saying that Zhao (1) says his patents are only for “credit (not for economic reasons)” and (2) hasn’t filed an IPR disclosure. These counterarguments are, however, irrelevant to the clear text of the BCP 79 requirements at issue.

As for the fixes: The first fix, regarding the first BCP 79 requirement at issue, would invoke BCP 79’s procedure to make an exception to that requirement. This procedure requires documenting a “very good reason” for the particular exception, and then having this reason “agreed to through IETF consensus”. None of this has happened: there hasn’t even been the basic admission that this procedure is required.

The second fix simply doesn’t work. It fails to address the specific BCP 79 requirements at issue; it’s another way of ignoring these requirements.

The third fix, regarding the second BCP 79 requirement at issue, is to take the document off the standards track. This has not been invoked.

5 Handling by the working-group chair

One of the draft authors sent email dated 15 Apr 2025 10:49:09 -0400 (https://mailarchive.ietf.org/arch/msg/spasm/0B8ADZDzKFcEnioldKb2q2OZ0OM/) saying “I believe this version addresses all of WGLC comments”. WGLC refers to “working group last call”. It is not true that this version addresses all of the WGLC comments. F1

I sent email dated 16 Apr 2025 16:29:46 -0000 (https://mailarchive.ietf.org/arch/msg/spasm/7JqwocYcfHFlHaStdc-0QawM0ok/) saying “No, the draft still doesn’t address various objections summarized here: https://cr.yp.to/2025/bcp-79-issues.html”. I also pointed to where the objections had been stated on list in response to WGLC (working-group last call):

- https://mailarchive.ietf.org/arch/msg/spasm/BTi8HqpFVpp_jv8keqr7cH5FfrE/
- https://mailarchive.ietf.org/arch/msg/spasm/zaRuZPUFmwg94y4FLgaib501CkI/
- https://mailarchive.ietf.org/arch/msg/spasm/U5pf3tPaBsmY4sth36bJg9gpGL4/
- https://mailarchive.ietf.org/arch/msg/spasm/zxNXERu9umB907mt_1OAfIvxB7o/
- https://mailarchive.ietf.org/arch/msg/spasm/PM4gQ_y0giQZct5LIqhyGhqF7dY/
- https://mailarchive.ietf.org/arch/msg/spasm/CmQLOuZxKHthamUuruNPcn95YQI/

- con: the draft does not comply with BCP 79 saying “An IETF consensus has developed that no mandatory-to-implement security technology can be specified in an IETF specification unless it has no known IPR claims against it or a royalty-free license is available to implementers of the specification”
  - con: can’t implement draft without implementing Kyber
    - fix: modify draft to allow alternatives to Kyber
    - pro: implementation of this spec is completely voluntary, ergo nothing in the spec is mandatory to implement (comment) (comment) (comment)
      - con: that position would make this BCP 79 rule useless (comment) (comment)
  - con: Zhao claiming “Kyber is covered by our patents” is a known IPR claim regarding Kyber
    - pro: Zhao hasn’t filed an IPR disclosure
      - con: BCP 79 says “no known IPR claims”, not “no known IPR claims for which the disclosure procedures of the document were followed”
    - pro: Zhao wrote patents are only for “credit (not for economic reasons)”
      - con: that’s irrelevant to this BCP 79 criterion
      - con: researchers normally say this; this doesn’t trigger estoppel and doesn’t stop them from asking for money (Ding asked Google for money re New Hope)
  - pro: will be good enough if there’s a royalty-free license before RFC publication, so WG can ignore this issue
    - con: BCP 79 assigns responsibility to WGs (“In general, IETF working groups prefer technologies with no known IPR claims or, for technologies with claims against them, an offer of royalty-free licensing”), not to subsequent publication stages
  - fix: BCP 79 has an exception procedure for this requirement: “It is possible to specify such a technology in violation of this principle if there is a very good reason to do so and if that reason is documented and agreed to through IETF consensus.”
    - con: procedurally, there has been no IETF-wide notification of a proposal to violate this BCP 79 principle
    - con: content-wise, there is no good reason to violate this principle, let alone a “very good reason”; should instead apply other fix above
  - fix: BCP 79 says “The IETF, following normal processes, can decide to use technology for which IPR disclosures have been made if it decides that such a use is warranted”
    - con: this is overridden by BCP 79’s subsequent text (quoted above) imposing a more specific requirement upon mandatory-to-implement security technology and imposing a higher bar for exceptions
- con: the draft does not comply with BCP 79 saying “The IETF must have change control over the technology described in any Standards Track IETF Documents in order to fix problems that may be discovered or to produce other derivative works”
  - con: BCP 79 continues by saying it isn’t prohibiting proprietary cryptography, but requires negotiations with the patent holders to ensure change control, as in RFC 1790 and RFC 2339
  - con: the available edited license excerpts for Kyber say “any modification, extension, or derivation of the parameters of the PQC ALGORITHM, is not an implementation or use of the PQC algorithm”
  - fix: don’t put document on standards track
  - pro: the document specifies ML-KEM only by reference
    - con: that position amounts to eliminating this BCP 79 rule
  - pro: without change control over ML-KEM, IETF can handle problems with ML-KEM by deprecating ML-KEM
    - con: that position amounts to eliminating this BCP 79 rule

Figure 1: Arguments and counterarguments regarding the violation of these two BCP 79 rules.

I had also mentioned previously on the WG mailing list that “various KEMs other than Kyber are used for patent reasons”, and I had explained the patent problems before that in considerable detail in other venues such as IETF’s general security mailing list (saag@ietf.org), but in any case the objections were stated on the spasm@ietf.org list in detail during WGLC.

One of the WG chairs (Russ Housley) sent email dated 16 Apr 2025 16:40:36 -0400 (https://mailarchive.ietf.org/arch/msg/spasm/SH6NmKuFcf8wytTvO6OMZPqY8F8/) repeating the claim that “this document is not specifying a mandatory to implement algorithm” (while ignoring my previously stated objection to that) and saying “I have explicitly asked whether the possible IPR related to ML-KEM is a concern. You are the only one to voice a concern” (which is not true—see, e.g., https://mailarchive.ietf.org/arch/msg/spasm/_aBRUG1mq3zd1wvanJimtLjEh7A/—and in any event is not a condition in the BCP 79 provisions at issue).

The chair then sent email dated 17 Apr 2025 08:37:23 -0700 forwarding one document to an area director (AD) for publication after IESG consideration (and then email dated 22 Apr 2025 09:51:11 -0700 similarly forwarding the other document).

6 Handling by the area director

I sent email dated 18 Apr 2025 00:40:20 -0000 (https://mailarchive.ietf.org/arch/msg/spasm/dMsFLzKwcEwowiw5uJdphOOJR6Q/) explaining what was wrong with the WG-chair response, and concluding as follows: “Seeing the chairs now forwarding this draft for publication tells me that we’re now at the ‘disagreement cannot be resolved in this way’ part of RFC 2026, Section 6.5.1, so I’m bringing this matter to the attention of the AD, and I’m hereby requesting that the AD invoke appropriate dispute-resolution procedures under Section 6.5.1.”

The relevant paragraphs of BCP 9 (RFC 2026) are as follows:

> A person who disagrees with a Working Group recommendation shall always first discuss the matter with the Working Group’s chair(s), who may involve other members of the Working Group (or the Working Group as a whole) in the discussion.
>
> If the disagreement cannot be resolved in this way, any of the parties involved may bring it to the attention of the Area Director(s) for the area in which the Working Group is chartered. The Area Director(s) shall attempt to resolve the dispute.
>
> If the disagreement cannot be resolved by the Area Director(s) any of the parties involved may then appeal to the IESG as a whole. The IESG shall then review the situation and attempt to resolve it in a manner of its own choosing.
>
> If the disagreement is not resolved to the satisfaction of the parties at the IESG level, any of the parties involved may appeal the decision to the IAB. The IAB shall then review the situation and attempt to resolve it in a manner of its own choosing.

Note that the uncontrolled discretion here (e.g., “manner of its own choosing”) is a due-process violation, as is the lack of any procedural constraints on the AD. A1

I sent followup email dated 18 Apr 2025 13:15:18 -0000 (https://mailarchive.ietf.org/arch/msg/spasm/tyXrEAglcUDZfGD3rWmzP2yBRJ0/) summarizing the patent timeline and the BCP 79 provisions at issue, with essentially identical text to Sections 3 and 4 of this document.

The AD’s entire “attempt to resolve the dispute”, beyond confirming receipt, consisted of email dated 25 Apr 2025 12:21:48 -0400 (https://mailarchive.ietf.org/arch/msg/spasm/FqgsTSZa0qCOdsloGOx3ScySmKA/) concluding—on the basis of the reasons reviewed below, ignoring various arguments already presented—that “no corrective action is warranted”. The specific reasons that the AD stated for this conclusion were as follows:

- First, the AD claimed that the “working group concluded that there is not an active IPR disclosure for formal consideration”.

  The phrases “active IPR disclosure” and “formal consideration” are ambiguous and do not appear in BCP 79. Also, attributing a position to the WG requires that position to have WG consensus established after being specifically brought to the WG for last call, but the AD provided no URL justifying this. **F2**

  As I had already pointed out (with no response), the first BCP 79 provision says “no known IPR claims”, not “no known IPR claims for which the disclosure procedures of the document were followed”. There is indisputably a known IPR claim from Zhao regarding Kyber. The fact that Zhao hasn’t followed BCP 79’s disclosure procedures is irrelevant to this BCP 79 provision. (It’s also irrelevant to the second BCP 79 provision, the change-control requirement.) **I1**

- Second, the AD claimed that the way that these drafts mandate Kyber does not meet the “mandatory to implement” part of the first BCP 79 provision, since *other* specifications don’t mandate usage of these drafts.

  As I had already pointed out (with no response), the question posed by this BCP 79 text (“no mandatory-to-implement security technology can be specified in an IETF specification unless . . . ”) is whether the specification mandates the technology. Misrepresenting the question as whether *something else mandates the specification* would make this BCP 79 rule useless. **I2**

- Third, regarding the second BCP 79 provision at issue, the AD claimed that the BCP 79 change-control requirement “refers to the content of this document only, not any normatively referenced algorithms”.

  This is contrary to both the text and purpose of this BCP 79 provision. Here is the provision again: “The IETF must have change control over the technology described in any Standards Track IETF Documents in order to fix problems that may be discovered or to produce other derivative works.”

  It doesn’t matter whether a technology is described by reference to another document or by repeating the contents of that document: either way, it is part of what the standard is describing, and IETF *must* have change control.

  As I had already pointed out, making an exception for technology described by reference amounts to eliminating this BCP 79 rule. *Any* standard would be able to factor out patented technology into a separate informational document cited as a normative reference. There was no response to this; that’s a due-process violation. **A2**

  The AD also quoted BCP 79 saying the following: “Note that there is no inherent prohibition against a Standards Track IETF Document making a normative reference to proprietary technology. For example, a number of IETF standards support proprietary cryptographic transforms.” This is not making an exception to the change-control rule; it is observing that the change-control rule is not inherently prohibiting proprietary technology.

  Within the broad area covered by the Ding patent, NIST has a license *only* for *exactly* NIST’s standard version of ML-KEM. The license explicitly forbids changes. IETF therefore does not have change control over the technology described in these drafts: in particular, for each draft, the description incorporates ML-KEM (by reference), and IETF cannot modify ML-KEM without violating Ding’s patent. This lock-in is very different from the situation of a narrow patent where changing to a different technology is simply outside the patent holder’s control. **I3**

- Finally, regarding the false (still not withdrawn) “addresses all of WGLC comments” claim, the AD said that there is no “requirement in the IETF process” to correct the statement.

  Misinformation about the status of objections is a due-process violation, and a violation of the specific “advised of the disposition” requirement. **A3**

7 Handling by the IESG

I filed a complaint with IESG by email dated 30 Apr 2025 20:22:28 -0000. I cc'ed spasm@ietf.org, and requested that all discussion be carried out there, including discussion of this matter among IESG members.

Procedurally, I stated three independent reasons for requesting IESG attention to this matter: an appeal provision in BCP 9 (RFC 2026), Section 6.5.1; Section 6.5.2 saying that IESG "is charged with ensuring that the required procedures have been followed, and that any necessary prerequisites to a standards action have been met"; and the obligations that antitrust law places upon standardization organizations. I noted an ambiguity in the first provision: "It is not clear that the 'cannot be resolved by the Area Director(s)' text in BCP 9 includes situations where the Area Director decides to take one side without engaging with what the other side said. However, using this as a reason to bar an appeal would violate the legal requirement of an appeals process."

I posted the complaint at https://cr.yp.to/2025/20250430-bcp-79.pdf, and then at https://cr.yp.to/2025/20250501-bcp-79.pdf after correcting a typo. The contents of the complaint were essentially identical to Sections 1, 2, 3, 4, 5 and 6 above.

IESG, without permission, posted a modified version of the complaint under my name, claiming that this modified version was the "Text contents" of the complaint. Here is an example of the modifications:

- Figure 1 has a clear structure, in particular with two items at the top level, namely the two BCP 79 provisions at issue.
- IESG's modified version has a dozen items at the top level.

I have issued a takedown notice to IESG regarding the modified version. IESG has not responded, so I have issued a formal takedown notice to IETF LLC.

The IETF chair sent email dated 22 May 2025 19:17:28 -0700 announcing an IESG response, namely https://datatracker.ietf.org/group/iesg/appeals/artifact/134. IESG kept its discussion secret, violating IETF LLC's claim that "IETF activities are conducted with extreme transparency, in public forums". I4

Regarding content, IESG's response began by misrepresenting the topic of the complaint: F3

```
The IESG received an appeal from Daniel Bernstein on May 1, 2025 for the
decisions of the LAMPS Working Group ("WG") Chairs and the responsible Area
Director ("AD") that declared WG consensus on
draft-ietf-lamps-kyber-certificates and draft-ietf-lamps-cms-kyber.
```

My complaint had started as follows: "This is a complaint to the Internet Engineering Steering Group (IESG) regarding recent violations of two provisions of BCP 79 (RFC 8179)." My complaint had identified the specific BCP 79 provisions at issue (see Section 2 for full quotes, and Section 4 for application to the situation at hand):

- the "no known IPR claims" requirement for "mandatory-to-implement security technology":
- the "change control" requirement.

These are not stated as requirements that can be overridden by "WG consensus". On the contrary, the first requirement sets a higher bar for exceptions: "It is possible to specify such a technology in violation of this principle if there is a very good reason to do so and if that reason is documented and agreed to through IETF consensus." There has been no attempt to invoke this procedure; furthermore, the second requirement does not allow such exceptions. See Figure 1.

IESG's response continued by misrepresenting the stated justification for the complaint: F4

```
The stated reasons for this appeal are perceived IPR issues and presumed
```

> restrictions on accepting technologies that might be covered by discriminatory IPR.

IESG had repeated my title of "Complaint regarding BCP 79 violations" (while editing the title, adding "in the LAMPS WG"). However, by writing "presumed restrictions", IESG was telling the reader that the complaint was inventing restrictions. Furthermore, by writing "perceived IPR issues", IESG was telling the reader that there was some relevant dispute about the patent facts. Whatever IESG's position might be, it is simply wrong for IESG to be describing this as the "stated reasons" for the appeal.

IESG then stated various forms of refusing the complaint:

> The IESG has concluded that there were no process failures by the WG, WG Chairs, or the responsible AD.
>
> The appeal is denied.
>
> Appeal response from the IESG
>
> The IESG has reviewed the matter and affirms the approach taken by the LAMPS WG Chairs and the responsible Area Director.
>
> Deb Cooley, responsible AD for the LAMPS WG, did not take part in the processing of this appeal by the IESG.

IESG continued by exaggerating the complaint's conclusions about ML-KEM's eligibility for standardization: **F5**

> IPR claim
>
> IESG Understanding of Appellant's Position
>
> The appellant asserts that there exists an IPR claim rendering the Module-Lattice-Based Key-Encapsulation Mechanism (hereinafter "ML-KEM"), a cryptographic technology, ineligible for standardization under the provisions of BCP 79, yet draft-ietf-lamps-kyber-certificates and draft-ietf-lamps-cms-kyber have been advanced to the IESG for publication.

My complaint did not claim that ML-KEM was "ineligible for standardization". On the contrary, extending the drafts to provide alternatives to ML-KEM, and negotiating change-control agreements, would allow the drafts to move forward in full compliance with BCP 79.

IESG continued by *partially* acknowledging that there was an allegation of BCP 79 violations:

> The appellant cites Section 7 of RFC8179/BCP79, "An IETF consensus has developed that no mandatory-to-implement security technology can be specified in an IETF specification unless it has no known IPR claims against it or a royalty-free license is available to implementers of the specification."

The facts go beyond this acknowledgment in two ways. First, the complaint was pointing to two different provisions of BCP 79, but here IESG was pointing to only one of the provisions (setting the stage for mixing up the requirements of the two provisions—see below). Second, the complaint wasn't merely citing these provisions; these BCP 79 provisions are the *sine qua non* of the complaint.

IESG could have simply said "this is a complaint alleging violations of the two BCP 79 provisions quoted below" and continued by addressing the merits of those complaints. Instead IESG threw up a smokescreen ("WG consensus"; "perceived" patent issues; "presumed" restrictions; "ineligible for standardization"; etc.). As noted above, misinformation about the status of objections is a due-process violation; this applies equally to IESG. **A4**

IESG continued with a “Timeline of Key Events”, which I won’t comment upon here beyond noting that it has fewer facts and fewer links than the complaint.

IESG then provided a “response” that ignored various objections already stated in the complaint, for example in Figure 1. This lack of response is a due-process violation. **A5**

Specifically, IESG wrote the following:

> `IESG Response`
>
> `Section 5.1.3 of RFC8179 describes the IETF processes for handling third party IPR disclosures. Section 5.3 of RFC8179 provides normative guidance on the mechanism for disclosure of IPR for the IETF to consider. The IESG has confirmed that at the time of this appeal response, neither the appellant, nor anyone else, filed an IPR disclosure for ML-KEM linked to draft-ietf-lamps-kyber-certificates or draft-ietf-lamps-cms-kyber in the datatracker.`

This is repeating the “Zhao hasn’t filed an IPR disclosure” argument from Figure 1, while ignoring the objection on point from Figure 1: “BCP 79 says ‘no known IPR claims’, not ‘no known IPR claims for which the disclosure procedures of the document were followed’ ”. **I5**

The suggestion that I was required to file an IETF IPR disclosure is incorrect. The suggestion that an IETF IPR disclosure is a prerequisite for this BCP 79 provision is also incorrect.

> `Despite the absence of a formal IPR disclosure, the IESG found that this potential IPR claim was raised in the LAMPS WG during the WG Last Calls for both documents, to include the WG Chair explicitly highlighting it. Even with awareness of this claim, the WG still found rough consensus to advance these documents to publication consistent with the WG processes for Last Call in Sections 3 and 7.4 of RFC2418 and Section 7 of RFC8179.`

Recall from Section 1 that, under antitrust law, consensus requires general agreement; fair consideration of each comment; a process of attempting to resolve each objection; and documentation—for any objection that was not resolved but that was instead overridden by general agreement—of why that objection was overridden. (Also, the law does not recognize “rough consensus” as a substitute for consensus.)

For example, consider again the objection saying that “BCP 79 says ‘no known IPR claims’, not ‘no known IPR claims for which the disclosure procedures of the document were followed’ ”. The law requires (1) fair consideration of this objection; (2) a process of attempting to resolve the objection; and (3) documentation—if this objection was not resolved but was instead overridden by general agreement—of why the objection was overridden.

None of this took place. Instead there was a generic call for consensus on moving the document forward. There is no documentation showing why this specific objection was overridden; what the records indicate is that the objection was simply ignored. Similar comments apply to the other objections covered in the complaint. **A6**

Furthermore, the claim of consistency with “RFC8179” (BCP 79) is incorrect. BCP 79 sets a high bar for exceptions to the no-known-IPR-claims requirement: “It is possible to specify such a technology in violation of this principle if there is a very good reason to do so and if that reason is documented and agreed to through IETF consensus.” Again, there has been no attempt to invoke this procedure. See Figure 1. **I6**

> `In particular, the appeal stated that the WG Chair’s conclusion on the appellant being the only one to have this potential IPR concern was wrong, as there was one more participant that had "concerns" per this WG Last Call feedback. While`

> the appellant is correct that this participant showed "concern", the participant nevertheless indicated support for the document going forward.

This is wildly misrepresenting the procedural status of a parenthetical remark from the complaint.

Specifically, the complaint had included the following paragraph: “One of the WG chairs (Russ Housley) sent email dated 16 Apr 2025 16:40:36 -0400 (https://mailarchive.ietf.org/arch/msg/spasm/SH6NmKuFcf8wytTvO6OMZPqY8F8/) repeating the claim that ‘this document is not specifying a mandatory to implement algorithm’ (while ignoring my previously stated objection to that) and saying ‘I have explicitly asked whether the possible IPR related to ML-KEM is a concern. You are the only one to voice a concern’ (which is not true—see, e.g., https://mailarchive.ietf.org/arch/msg/spasm/_aBRUG1mq3zd1wvanJimtLjEh7A/—and in any event is not a condition in the BCP 79 provisions at issue).”

IESG has now admitted that the WG chair’s “only one to voice a concern” statement is false. But the number of people raising a concern has always been a red herring raised by the WG chair. The BCP 79 provisions at issue aren’t triggered by the number of people voicing a concern. I7

> Per Section 2 of RFC8179, the IESG repeats that "the IETF will make no determination about the validity of any particular IPR claim."

Irrelevant. BCP 79 says “no known IPR claims”, not “no known valid IPR claims”.

> Furthermore, "the IETF, following normal processes, can decide to use technology for which IPR disclosures have been made if it decides that such a use is warranted."

This is repeating another argument from Figure 1, while ignoring the objection on point in Figure 1, namely “this is overridden by BCP 79’s subsequent text (quoted above) imposing a more specific requirement upon mandatory-to-implement security technology and imposing a higher bar for exceptions”. I8

> While no formal IPR claim was filed to consider, the LAMPS WG was informed of this potential IPR claim, and still found rough consensus during WG Last Call to proceed with publication.

Covered above.

> The IESG also notes that the handling of this potential IPR claim was documented in the shepherd write-up of draft-ietf-lamps-kyber-certificates and the shepherd write-ups of draft-ietf-lamps-cms-kyber. As such, it will be available for review and consideration during the IETF Last Call.

This “note” seems to be repeating the timeline aspect of the “will be good enough if there’s a royalty-free license before RFC publication, so WG can ignore this issue” argument from Figure 1, while ignoring the objection on point in Figure 1, namely “BCP 79 assigns responsibility to WGs (‘In general, IETF working groups prefer technologies with no known IPR claims or, for technologies with claims against them, an offer of royalty-free licensing’), not to subsequent publication stages”. I9

> "Mandatory-To-Implement" claim
>
> IESG Understanding of Appellant’s Position
>
> The appellant asserts that, since ML-KEM is a required dependency of draft-ietf-lamps-kyber-certificates and draft-ietf-lamps-cms-kyber, it renders

> ML-KEM mandatory-to-implement (MTI). As change control of ML-KEM is the purview of US NIST, the appellant asserts that these documents violate Section 7 of RFC8179/BCP79, which states "The IETF must have change control over the technology described in any Standards Track IETF Documents in order to fix problems that may be discovered or to produce other derivative works."

It's remarkable how many major errors IESG packed into this paragraph. Here are the facts.

First, "mandatory-to-implement" is ambiguous if one doesn't say *what's* issuing the mandate. My complaint was completely clear about the distinction between

- **a technology mandated by a specfication** and
- **something else requiring usage of that specification**.

Sample quote from my complaint: "As I had already pointed out (with no response), the question posed by this BCP 79 text ('no mandatory-to-implement security technology can be specified in an IETF specification unless . . . ') is whether the specification mandates the technology. Misrepresenting the question as whether *something else mandates the specification* would make this BCP 79 rule useless."

IESG isn't clearly distinguishing these concepts (see below). But my complaint *did* clearly distinguish these concepts. IESG was wrong in attributing an ambiguous "mandatory-to-implement" claim to my complaint. **F6**

Second, NIST does not hold any of the patents mentioned in my complaint. NIST bought a license under Ding's patent *for exactly the standardized version of ML-KEM*, according to the edited license excerpts posted by NIST. Change control remains with Ding, the patent holder.

So IESG was wrong in claiming that "change control of ML-KEM is the purview of US NIST". **F7**

Third, while "mandatory-to-implement" is relevant to the "no known IPR claims" requirement in Section 7 of BCP 79, it's irrelevant to the change-control requirement in Section 8 (not 7) of BCP 79. Here are the two different requirements again (see Section 2 of this complaint for more context):

- "An IETF consensus has developed that no mandatory-to-implement security technology can be specified in an IETF specification unless it has no known IPR claims against it or a royalty-free license is available to implementers of the specification."
- "The IETF must have change control over the technology described in any Standards Track IETF Documents in order to fix problems that may be discovered or to produce other derivative works."

The no-known-IPR-claims requirement is for technology mandated by a spec; the change-control requirement is for any spec on the standards track. So IESG was wrong in lumping the change-control requirement into a discussion of what's "mandatory-to-implement". **I10**

> IESG Response
>
> Draft-ietf-lamps-kyber-certificates and draft-ietf-lamps-cms-kyber specify optional extensions to the Internet X.509 Public Key Infrastructure Certificate Profile (X.509) and Cryptographic Message Syntax (CMS). While both documents cite ML-KEM as a normative reference, the concepts of "mandatory-to-implement" and normative reference are not synonyms.

It's correct that a spec can cite normative references without mandating implementation of those. For example, consider a spec that allows two different options X and Y, that leaves it up to the implementor whether to implement X or to implement Y, and that cites other documents for implementation details of X and Y. This spec needs both X and Y as normative references even though it isn't mandating either one.

This possibility was already covered in "fix: modify draft to allow alternatives to Kyber" in Figure 1. However, the current drafts aren't providing alternatives to Kyber. **I11**

> Citing ML-KEM normatively does not bestow any sort of mandatory status or otherwise compel any developer to implement, enable, or otherwise support ML-KEM to be able to use X.509 or CMS. Put more simply, these documents say, in effect: If one is going to add ML-KEM support to an X.509/CMS implementation, this is the IETF's standard method of doing so. The decision explicit in the first word of that statement ("If") contradicts any notion of "mandatory", and what is being standardized is the link between the X.509/CMS and ML-KEM, not ML-KEM itself.

This is repeating the "implementation of this spec is completely voluntary, ergo nothing in the spec is mandatory to implement" argument from Figure 1, while ignoring the objection on point from Figure 1, namely "that position would make this BCP 79 rule useless".

The rule at issue—"An IETF consensus has developed that no mandatory-to-implement security technology can be specified in an IETF specification unless it has no known IPR claims against it or a royalty-free license is available to implementers of the specification"—is a policy constraint on any security technology mandated by an IETF spec. It isn't a content-free statement that new specs aren't mandated by anything else.

Ultimately many IETF specs do end up being mandated by, e.g., purchasing requirements naming particular RFCs (never mind the usage of RFC compliance for marketing). Companies pay people for IETF participation because of the influence that they wield through this process. So focusing on the situation of a new spec not being mandated yet by anything else would be ignoring long-term damage in favor of a content-free temporary situation. Anyway, this isn't what the text of BCP 79 does. The text "no mandatory-to-implement security technology can be specified in an IETF specification unless . . . " is asking whether that specification mandates implementation of a security technology, not whether something else mandates usage of that specification.

> Requiring change control of every normative reference would essentially mean the IETF could not have a normative reference to a document it did not author.

Again, the change-control requirement is a separate requirement in BCP 79, *not* triggered by whether a spec has "mandatory-to-implement security technology". IESG provided a remarkably short discussion of change control, in part through its overall failure to systematically quote and respond to the objections at hand and in part specifically by conflating these two different BCP 79 requirements.

Anyway, IESG's claim here is factually incorrect. IESG is misrepresenting BCP 79 in general, and the change-control requirement in particular, while ignoring the specific problem triggered by ML-KEM's unusual licensing arrangements. **F8**

BCP 79 has title "Intellectual Property Rights in IETF Technology". It explicitly removes copyrights (and trademarks) from its scope, saying that those are covered in RFC 5378, "including the right of the IETF and IETF Participants to publish and create derivative works of those Contributions".

When BCP 79 says "change control", it's talking about *patented technology* where usage needs permission from patent holders, not about *copyrighted text* where editing needs permission from the original authors. BCP 79 is saying that "the developer of patented or otherwise controlled technology may decide to hand over to the IETF the right to evolve the technology (a.k.a., 'change control')". BCP 79 is saying that this is mandated for "any Standards Track IETF Documents", so that IETF is able "to fix problems that may be discovered or to produce other derivative works". See Section 2 for the full quote.

Does this policy lead to IESG's horror scenario "IETF could not have a normative reference to a document it did not author"? Of course not. This policy puts no constraints on unpatented technology.

> Section 8 of RFC 8179 explicitly states that "Note that there is no inherent prohibition against a Standards Track IETF Document making a normative reference to proprietary technology. For example, a number of IETF standards support proprietary cryptographic transforms."

Here IESG is simply ignoring what the complaint had already said about this paragraph: “this is not making an exception to the change-control rule; it is observing that the change-control rule is not inherently prohibiting proprietary technology”.

> Notwithstanding the conclusions of the IPR claims section, this claim fails on its merits.

See above.

> Background Analysis of the Documents
>
> Draft-ietf-lamps-kyber-certificates specifies conventions for using ML-KEM in X.509 Public Key Infrastructure. Draft-ietf-lamps-cms-kyber specifies conventions for using ML-KEM with the CMS. Collectively they define these conventions by building on prior Public Key Infrastructure (PKIX) and CMS specifications such as RFC3565, RFC5083, RFC5280, RFC5912, RFC5652, RFC5958, and RFC9629.
>
> These PKIX RFCs and those that update them do not provide normative language on which algorithm is mandatory to implement. This lack of guidance makes implementing ML-KEM optional in the X.509 Public Key Infrastructure.
>
> Additionally, the referenced CMS specifications do not provide normative language on which algorithm is mandatory to implement. In particular, the base CMS specification, Section 1.1.2 of RFC5652 states that "This specification does not require the implementation of any particular algorithms. Rather, protocols that rely on the CMS are expected to choose appropriate algorithms for their environment." Furthermore, Section 2 of draft-ietf-lamps-cms-kyber explicitly begins with "the ML-KEM algorithm MAY be employed ..." and then enumerates the possible data structure in CMS. This guidance makes implementing ML-KEM optional for CMS.

Here IESG is again ignoring the BCP 79 question (for the first BCP 79 provision at issue), namely whether a spec is mandating a security technology. Instead IESG is substituting an irrelevant question, namely whether something else requires usage of this spec.

> Standing of a Blog Post
>
> The IESG notes that the appellant cites a sentence from an IETF Administration LLC blog post in several forums, including this appeal: "IETF activities are conducted with extreme transparency, in public forums". The appellant appears to interpret that text as normative guidance which requires any parties discussing their request to do so only in public forums, and prohibiting private discussion.
>
> The IESG is clarifying that this interpretation is incorrect. This blog post is a narrative summary of existing RFCs speaking in generalities, and provides no new normative guidance for the IETF. If there is specific concern about normative communication practices, please cite an appropriate RFC.

Formally, IETF is an activity by IETF LLC, a subsidiary of ISOC. IESG, in turn, is an IETF committee. So IESG members are acting as agents of IETF LLC.

IETF LLC has issued an “IETF Administration LLC Statement on Competition Law Issues” making a variety of specific claims about how IETF works, as part of saying “IETF processes and procedures are particularly well-suited to mitigate competition law risks". But IESG claims that, no, this is just a "blog post" that IESG isn't obliged to follow. Announcing rules and then not following those rules is a due-process violation. A7

Concretely, IESG members seem to think that it's just fine that IESG's deliberations regarding this matter (perhaps also involving other parties) are secret. But this is contradicting the IETF LLC statement that "IETF activities are conducted with extreme transparency, in public forums", and thus also undermining the IETF LLC statement that "IETF processes and procedures are particularly well-suited to mitigate competition law risks". Even if IETF LLC doesn't care whether its claims match the reality of how IETF operates, IESG members should care about not putting themselves into a risky legal position.

Furthermore, RFC 2026 (BCP 9), "The Internet Standards Process – Revision 3", includes the following requirements (which I hadn't quoted in my complaint to IESG, but it's not plausible that IESG is unfamiliar with such basic rules):

> 8. NOTICES AND RECORD KEEPING
>
> Each of the organizations involved in the development and approval of Internet Standards shall publicly announce, and shall maintain a publicly accessible record of, every activity in which it engages, to the extent that the activity represents the prosecution of any part of the Internet Standards Process. For purposes of this section, the organizations involved in the development and approval of Internet Standards includes the IETF, the IESG, the IAB, all IETF Working Groups, and the Internet Society Board of Trustees.
>
> ...
>
> The formal record of an organization's standards-related activity shall include at least the following:
>
> - the charter of the organization (or a defining document equivalent to a charter);
> - complete and accurate minutes of meetings;
> - the archives of Working Group electronic mail mailing lists; and
> - all written contributions from participants that pertain to the organization's standards-related activity.

Certainly any email contributions from IESG participants regarding this matter "pertain to the organization's standards-related activity". Any spoken contributions have to be reflected in "complete and accurate minutes of meetings". More broadly, there has to be a "publicly accessible record" of "every activity" that is "part of the Internet Standards Process".

IETF LLC's claim that "IETF activities are conducted with extreme transparency, in public forums" is in line what BCP 9 requires. But IESG claims to be free to carry out secret deliberations, and, as this incident illustrates, does in fact carry out secret deliberations. I12

> Conclusions
>
> The IESG determines that:
>
> The potential IPR claim described in this appeal was raised in the LAMPS WG, considered during WG Last Call, and the WG chairs and responsible AD appropriately declared rough consensus from the WG Last Calls that enabled advancement of drafts. The "mandatory-to-implement" claim raised in this appeal is not applicable to these documents.
>
> The appeal is denied.

See above.

8 Balance of interests

The centerpiece of this complaint is the BCP 79 provisions being violated, but it's also helpful to keep in mind the underlying problems caused by patents.

Most potential uses of public-key cryptography in the 20th century were held back by the DH and RSA patents. For example, in May 1991, Mark Riordan released free "rpem" encryption software (https://groups.google.com/g/sci.crypt/c/UUPxWhTiQrM/m/HWGWbwGhvOgJ) using the Rabin public-key cryptosystem: The RSA patent holders sent him a letter claiming that he was infringing the RSA patent. Whether or not the claim was correct, he couldn't afford to fight a patent lawsuit, so he withdrew the software (https://groups.google.com/g/sci.crypt/c/gFImCh6qmAs/m/9zKEAfbfdTIJ). The RSA company built a large business selling RSA to companies that could afford the patent fees, but the bottom line was that most applications that could have used RSA (or Rabin) were left unprotected, to the detriment of the end users.

In July 2016, Google rolled out an experiment with post-quantum cryptography. As part of its announcement (https://security.googleblog.com/2016/07/experimenting-with-post-quantum.html), Google wrote the following: "We explicitly do not wish to make our selected post-quantum algorithm a de-facto standard. To this end we plan to discontinue this experiment within two years, hopefully by replacing it with something better. . . . While it's still very early days for quantum computers, we're excited to begin preparing for them, and to help ensure our users' data will remain secure long into the future." Google announced a few months later that it was disabling the experiment and *not* replacing it with something else. What had happened in the meantime was that Ding had contacted Google to ask them for money under his patent. Again this was to the detriment of the end users: Google regressed to pre-quantum cryptography that will *not* remain secure long into the future.

Today Google and other large tech companies are again taking risks by rolling out Kyber. Will Zhao file a patent lawsuit? Will a Kyber patch be required for security reasons, allowing Ding to file a patent lawsuit because the patched version isn't covered by NIST's license?

We don't know at this point. What we do know is that many other companies are scared (see, e.g., "very worried about the patents" on page 5 of https://datatracker.ietf.org/meeting/116/materials/slides-116-pquip-patents-and-pqc-00 from 2023), especially small companies that can be put out of business by a patent lawsuit. The public evidence is only the tip of the iceberg: companies of all sizes often stay quiet about specific patents because they're concerned about being subjected to the triple-damages rule in patent law. (See, e.g., the policy reported in https://groups.google.com/a/list.nist.gov/g/pqc-forum/c/GODoD7lkGPk/m/6-dbCjmVBgAJ.)

Has this stopped Kyber rollout? No. Some companies haven't heard about the problems; some companies can afford to take patent risks. But the big picture is that—to the extent that the market for post-quantum encryption is artificially restricted to Kyber—competition in the market is limited, and the range of applications is limited. This is financially rewarding for some companies such as Google, but it's again to the detriment of the end users.

The public interest generally outweighs the interests of patent holders. So it makes sense that BCP 79 states a general preference for "technologies with no known IPR claims". BCP 79 upgrades this preference to a requirement whenever a spec mandates implementation of a security technology. BCP 79 also requires change control for all IETF standards-track technology, so that IETF is free to modify what it's doing.

What we're seeing in the incident at hand is very much the opposite of what BCP 79 requires. IETF, to the extent it's pushing forward with Kyber, is pushing users into a technology where there's a known IPR claim (from Zhao), with no free license under that claim. Even worse, any modification will crash into another known IPR claim (from Ding), because the NIST license is only for *exactly* what NIST has standardized. Instead of providing alternative mechanisms that entirely avoid the patent mess, IETF is acting as if BCP 79 doesn't exist.

The underlying problem here is that every level of IETF is dominated by large tech companies. For example, beyond the IETF chair (Roman Danyliw from CMU), here are the affiliations of the IAB members:

- Nokia (Matthew Bocci).
- Huawei (Dhruv Dhody).
- Fastly (Jana Iyengar).
- Cisco (Cullen Jennings).
- Cisco again (Suresh Krishnan).
- Ericsson (Mirja Kühlewind).
- Google (Warren Kumari).
- Comcast (Jason Livingood).
- Cloudflare (Mark Nottingham).
- Apple (Tommy Pauly).
- Huawei subsidiary Futurewei (Alvaro Retana). Huawei and Futurewei have caused some confusion by removing public mentions of their ties, but court proceedings such as https://storage.courtlistener.com/recap/gov.uscourts.nyed.500931/gov.uscourts.nyed.500931.34.0.pdf continue to show Futurewei's status as a subsidiary of Huawei.
- Huawei again (Qin Wu).

This is not a balance of interests. **A8**