1. Article #2 “state-of-the-art”:
    a. What specifically is meant by “Start of the Art”? The way this term is used does not make much sense as many of the documents that are considered state of the art of around 10 years old, which is old in tech (and security).
    b. Can a better term, or an updated description replace this term?
2. Article 4: Multi-level Assurance Product:
    a. CC:2022 (or the equivalent ISO), provides for multi-assurance evaluations where sub-components are evaluated at higher assurance than the product as a whole. How would the whole product be evaluated: at the Highest Assurance or individual components of the resulting TOE?
    b. Would this be considered High or Substantial?
3. Article 4: General:
    a. How are protection profiles (PPs) certified with respect to Substantial? Is it required to have a certified PP?
4. Article 4:
    a. There doesn’t seem to be any expectation of meeting traditional EALs for an evaluation. With no EAL level is present, does that mean it needs to be a PP? How about cPP?
    b. How does this meet a High? Could you have a high AVA_VAN but low everything else (compared to traditional EALs), or are the AVA_VAN levels still tracked to the traditional EALs?
    c. Are the ATE_IND/ALC_FLR SAR levels tied to the AVA_VAN level or are they independent?
5. Article 5:
    a. What is the process of defining an ITC Product Category?
    b. Once one is defined, how would PPs be added?
    c. Will ITC Product Categories be defined for Substantial, or only ever for High?
6. Article #7:
    a. Does this only apply to HIGH or does it also apply to SUBSTANTIAL?
    b. If it applies to SUBSTANTIAL, what are the applicable state-of-the-art documents?
7. Article #7 #4:
    a. Labs are supposed to share information to other labs? Contractual and Legal obligations will prevent a one lab from sharing confidential information to another lab. A vendor’s information (such as that contained within the evaluation report to the CB) is confidential to the lab (by NDA) and to the CB by virtue of need to complete the evaluation. Providing this information to a second lab, from the lab, violates legal agreements between the vendor and lab.
8. Article #8 6a:
    a. Is the website provided here supposed to be used as the link in the QR Code in Article #11?
9. Article #8 7

    a. The period of retention of 10 years seems to be prohibitively long. What is the rationale for that length of time? Is this an administrative problem/solution?
    b. This is also in conflict with Articles #41 & 42 which list 5 years after expiration, which is a long period already. Note that requiring the CB to maintain the report and certification documents make sense to be maintained, but not the vendor/ITSEF
10. Article #9 1e combined with Article #8 2:
    a. These imply that source code must be shared by Vendor with CB. While some level of sharing with the ITSEF is "common", sharing with the CB is likely to be very limited.
    b. When is source code "Necessary"?
    c. Is this required for Substantial or only for High?
11. Article #11:
    a. What is the requirement for inclusion of the mark across multiple documents? For example a CC configuration document that references other non-CC-specific documents? Are all the referenced documents required to have the mark, or only the CC-related one?
    b. Can the mark (and QR Code) be used on other documents? For example can it be used on the product website, marketing materials, etc?
    c. Where is the QR code supposed to point? The implication here is that this website may be something owned by the vendor, and would then need to be a long-lived URL (which is difficult generally for commercial products as sites are continually updated for marketing purposes).
    d. How long does the QRcode / related URL need to be maintained by the Vendor if it is a vendor website?
    e. Why wouldn't the URL go to the CB for authoritative confirmation? From there the vendor could then provide a link to the product website they maintain, and could provide updated links over time as the commercial website is updated.
    f. Does the QR Code reference a URL that goes to the CB, Vendor or some other authoritative source?
12. Article #12 1:
    a. Implies there is no consistency.
    b. There needs to be clarity on the length of certification. While there may be different terms, this doesn't provide any consistency as it is implied that the CB can decide how long an individual certificate will be for. There is no guarantee that 2 products in the same category need to be provided the same longevity based on this statement.
13. Article #13
    a. This should reference Article #26 in stating these are the triggers for a re-evaluation
14. Article #15 2a:
    a. How are PPs added to these lists?

   b. For Substantial, how can technical domains be established and PPs assigned to them? These would be technical domains not referred in Annex I

15. Article 17
    a. A mechanism needs to be defined certifying EUCC approved PPs
    b. Today most PPs are certified on first use, though others may be certified independently. What are the allowed methods for this?
16. Article #18:
    a. Clarification on the validity period for PPs. These statements seem somewhat contradictory to each other. Lifetimes are normally explicit time periods, not “lifetime” which is undefined
17. Article #21 & #22:
    a. Since these are clearly both for HIGH, are there any requirements for SUBSTANTIAL?
18. Article #25 2d:
    a. What is meant by a “complaint”? A complaint about what/who? This is repeated in several monitoring Articles, and is similarly undefined in each case. The object of the complaint can have a lot of impact about what the monitoring is reviewing. Complaints about vendor products would be about checking for vendor compliance, whereas complaints about the lab could be about checking for lab compliance with proper test procedures.
19. Article #25 3:
    a. Is the 5% sampling ONLY from those received within the last 12 months / calendar year? What about checks on products on the list older than that time period?
    b. Are products that undergo maintenance/updates within 12 months eligible to be sampled again (so say sampling a product at 6 months, it is updated and has the cert extended after 10 months, could it be sampled again in the next 12 months after the update)?
20. Article #27 2:
    a. What is the expected cooperation between Vendor and other bodies?
21. Article #30 3:
    a. There is no guarantee to know exactly who purchased the product or maintain ownership addresses? Many products are not sold directly to the customer from the vendor but through resellers.
    b. How would it be possible to notify purchasers in this case?
    c. Would a public notice on the vendor’s website be sufficient (where users could see this or possibly subscribe to product updates)?
    d. Is this specific to High or also Substantial?
22. Article #33 3:
    a. Why/Where did the very short 3 days for notification come from? Seems very short!
23. Article #33 3:
    a. Notifications can only take place after proper triage can be completed. Notifying everyone immediately of something that *may* be a problem is a dangerous undertaking prior to conclusion of problem. Not to mention that

vendors receive LARGE amounts of reports about problems, both listed as vulnerabilities and not (and not necessarily accurately labeled or understood by the reporting party). Without proper triage of the reported issue, notifications are largely meaningless.

24. Article #33:
    a. Does all of this apply to HIGH, SUBSTANTIAL or BOTH?
25. Article #35 2:
    a. What are defined as “appropriate security measures” for protecting the vulnerability information?
    b. How is the information delivered in a secure manner to the CB? While there are requirements about the vendor needing to have a way to receive information securely, there are no such requirements on the CB.
    c. How can vendors be assured that the information will be protected by the CB?
26. Article #35 3:
    a. How long before the CB comes back to the Vendor with a decision? What is considered a “reasonable time frame” given that the vendor is expected to meet specific deadlines for reporting and deploying patches. How does the CB decision process factor into those time frames?
    b. What is expected to happen if the vendor deploys the patch and the CB does not approve it? Is there a dispute resolution process? Does the vendor have additional time to understand the disagreement and either provide additional justification to the original position or time to generate a different patch (to be applied over/with the original one) to bring the product into compliance?
27. Article #36 general
    a. For vendors who perform regularly scheduled updates, how is remediation supposed to be handled? While the timelines involved may be relevant, when products have regular updates (such as quarterly or monthly), would the product(s) need to be in continual suspension and assessment so the patches can be continually reviewed (and how would this ever mean the product could be certified, since the changes are likely faster than the review/certification process).
28. Article #37 general
    a. While most vendors have an embargo period, there are times when 30 days is not sufficient to develop an update to resolve the vulnerability. It is not clear the conditions under which the embargo may be extended (what type of justification is sufficient). Further, this seems to apply to High, but what is the expectation for Substantial products?
29. Article #39 general
    a. What is the expectation for this for Substantial products? Is there a similar expectation of sharing among certification bodies, and if so, to what extent? Since the vendor does not have relationships with other CBs, it is difficult to understand how such sharing can be implemented that protects the company from potential exposure of the vulnerability such that it could lead to attacks prior to a fix.

30. Article #40
    a. What is the expectation of the publication of the vulnerability? Does the vendor have any say in the documentation provided about the vulnerability, or the ability to see what is proposed prior to posting?
31. Article #41, 2
    a. What is the reason for the ITSEF keeping all records for 5 years after the expiration of the certificate? This seems a very long time for maintaining that information by the lab for something that would have been completed (even for all maintenance updates) for a long period of time.
32. Article #42 2 & 3
    a. Retaining copies of all information submitted as part of an evaluation, 5 years after the expiration of the certification of the product, which may be as much as 10 years after the certification, is an unrealistic prospect for a commercial product. There is no commercially justifiable purpose for this retention except as an expense for the company.
    b. Similarly, for a commercial product, why would there be an expectation of keeping a specimen of the certified product? How many is sufficient? Is it expected that this is an “unboxed” unit such that it should be able to run as new (and what if it has degraded by age such that it is no longer able to work)? Or is the product expected to be maintained to the latest iteration (i.e. patches, updates, etc)? This is very unclear and how it would be justified to a commercial entity seems problematic.
    c. Under what conditions would the vendor be asked to make such records available? There is nothing here except “upon request” with no specification as to what may trigger this. Further, at what point would information for a no-longer-certified product be requested (and what would compel the vendor to comply since there is no certificate that can be “threatened”)?
33. Article 45:
    a. What is the transition plan for Mutual Recognition between SOG-IS, CCRA, ISO, etc. preventing members from having to pull out of their existing organization?
    b. What is the plan to ensure that vendors currently utilizing mutual recognition agreements that become void with EUCC that they will not need to perform multiple, separate evaluations in different countries (or regions) to have evaluated products accepted?