Comment #	Submitted By	Comment (include rationale)*
1	Mike Bursell, Executive Director, CCC	Confidential Computing, confidentiality and integrity
2	Mike Bursell, Executive Director, CCC	Attestation for output model tracking, attestation for training dat
3	Mike Bursell, Executive Director, CCC	Complementarity with other PETs and technologies
4	Mike Bursell, Executive Director, CCC	Cross-platform nature of CC
5	Mike Bursell, Executive Director, CCC	CC for cross-jurisdictional capabiltiies
6	Mike Bursell, Executive Director, CCC	Regulatory and standards work

7	Mike Bursell, Executive Director, CCC	Trustworthiness not an inherent property (Denning), but contextu

Suggested Change*
Confidential Computing is the protection of data in use by performing computation in a hardware-based, attested Trusted Execution Environment. It is one of a family of Privacy-Enhancing Technologies (PETs), and can provide confidentiality and integrity protections to workloads and data via hardware-based isolation, protecting data even from the owner and/or operator of the system on which processing is taking place. The industry body for Confidential Computing is the Confidential Computing Consortium, a Linux Foundation project with members ranging from start-ups to multi-nationals and based in countries around the world. [https://confidentialcomputing.io/wp-content/uploads/sites/10/2023/03/CCC-A-Technical-Analysis-of-Confidential-Computing-v1.3_unlocked.pdf], [https:
In Confidential Computing, an attestation is the validation of a hardware signed report (an “attestation report”) of the measurements of the Trusted Compute Base (TCB). This can be used to provide assurances as to the identity of both code (and/or training models) and input data and to tie this to known sets of production models and output data, also providing cryptographic assurances as to the confidentiality and integrity of the AI model and data provenance and "supply chain".
Confidential Computing allows the execution of standard computer code using enabled processing units (e.g. CPUs and GPUs). This means that it can be combined with other PETs to complement the properties they provide, or with other technologies in the lifecycle of AI applications.
Confidential Computing is a function of the use of Trusted Execution Environments (TEEs) are functionality provided by processing units (e.g. CPUs and GPUs). CPUs and GPUs with these capabilities are available from multiple vendors and are widely deployed in public clouds.
Given the ability of Confidential Computing to isolate computation and data from the owner or operator of the system hosting and performing the processing, it provides opportunities for organizations in one jurisdiction to collaborate with organizations in other jurisdictions and even to use computing resources in other jurisdictions whilst maintaining control of the confidentiality and integrity of the code, models and data.
As Confidential Computing is being adopted by industry, one way to speed take-up is by encouraging relevant regulatory and standards bodies to engage with the technology. The Confidential Computing Consortium provides a single point of contact for such bodies, and while the consortium is already working in this area, always welcomes work by government and other bodies to encourage regulatory and standards engagement.

It is important to note that trustworthiness is not an inherent property of a system, but highly context-specific, and must be tied to the expectations of the system and the use to which it will be put, as noted by Denning (1993, p.38). [Denning., D.E. (1993). A new paradigm for trusted systems. https://www.researchgate. net/publication/234793347_A_New_Paradigm_for_Trusted_Systems], [Bursell, Mike (2021). *Trust in Computer Systems and the Cloud*, Wiley, Hoboken, NJ.]

