Charter proposition I

Timing covert channels are used to exfiltrate confidential data using microarchitectural states as a medium for communications. These channels are particularly relevant in the context of microarchitectural attacks such as Spectre and Meltdown.
The Microarchitecture Side-Channel Resistant Instruction Spans Task Group (proposed short name: uSCR-IS TG) will define a small ISA extension to prevent malicious covert channels. More precisely, we will introduce a notion of side-channel resistant instruction spans, such that covert channels can be prevented across instruction spans by adapting the microarchitecture. Introducing instruction spans as an architectural feature makes it possible for higher-level program logic to declare that a sequence of instructions should be microarchitecturally isolated within a larger instruction stream (for example, a span of instructions that implement a cryptographic operation may be isolated to protect against side-channel attacks). The proposed RISC-V uSCR-IS TG will collaborate to produce:

1. A small ISA extension (possibly no more than one or two instructions, or only a new CSR).

Charter proposition II

2. A security guide: defining threat models, developing rationale, etc. -> intended for security engineers.
3. An implementation guide, focusing on the principles of microarchitecture design that enable protection against covert channels. -> intended for hardware engineers.
4. A proof-of-concept implementation, including both a prototype RISC-V core and compiler managing the necessary intrinsics.
5. A test strategy guide, including a test suite for common covert channels.

The TG will work with the appropriate Priv/Unpriv ISA committee, Architecture Review Committee, and Security HC to determine which parts of the work should follow the standard ISA specification process, Fast Track process, or non-ISA process, and how other recent policy or process changes may apply (such as the discussion around the use of hint instructions in CFI).