




# Security HC

4/13/2023





# Disclosures



# Agenda - 4-13-2023

- **Disclosures**
- **WorldGuard proposal discussion**
  - Tentative home -> M-mode iso TG (in RI SIG slot)
  - Some feedback from folks (Mark, Ravi, Ved, Dean, DavidA, Paul, Fabrice, Yann, Deepak)
  - Some folks have to still read the spec so we will resume discussion in M-mode isolation TG.
- **SIG, TG updates**
  - Sec Model TG - WIP on the domain isolation
    - P1 Domain isolation
    - P2 Secure and verified boot, updates (and required platform properties, behaviors)
      - Revise threat model and suggest countermeasures (and not implementation)
  - Need M-mode isol meetings to be held
  - RI SIG charter up-leveling
    - CFI, S-PMP stable
    - IO-PMP (working on error reaction to illegal accesses).
  - TC SIG
    - AP-TEE - using common NaCL SBI for memory sharing; binding unbinding IMSIC - API
      - Attestation - adds EAT for gathering measurements
      - Smmntt - will be moved to github to start tracking changes
    - Ap\_TEE\_IO - TG - formed