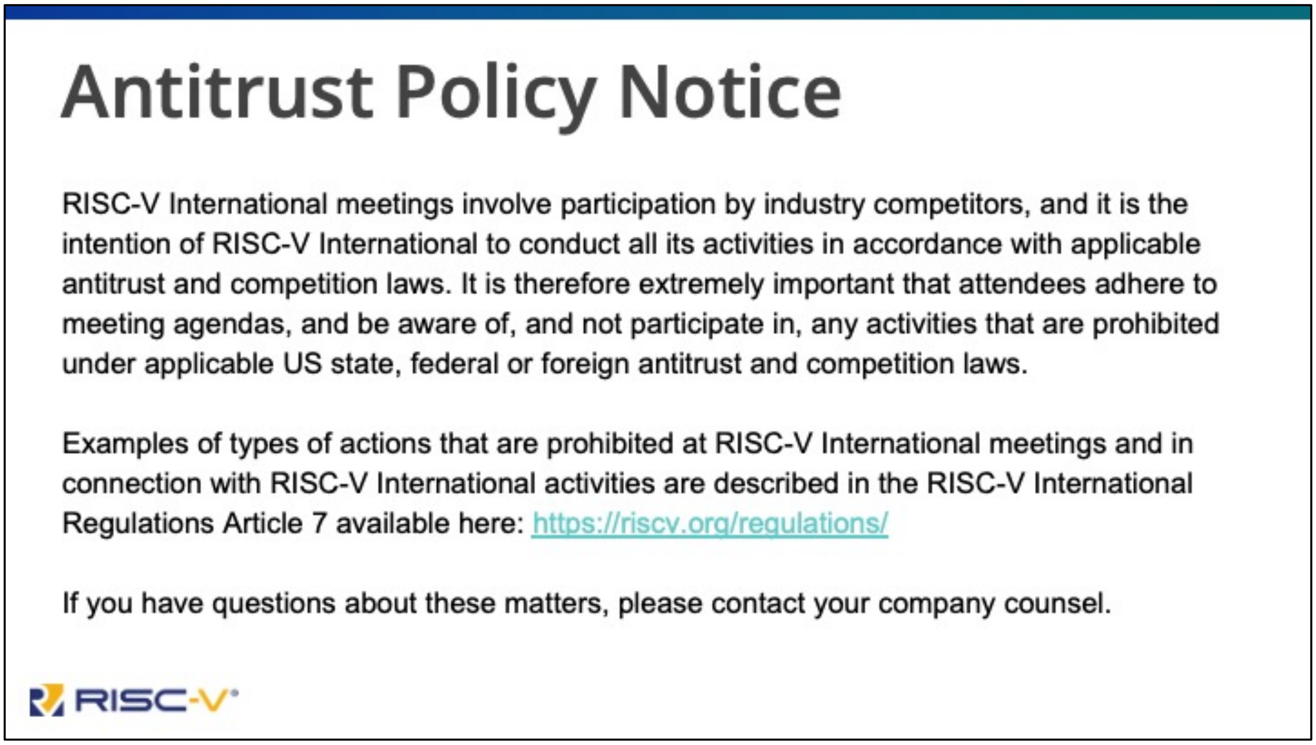
RISC-V®

Security HC

September 16, 2021

Meeting notes from the Security HC call, September 16, 2021

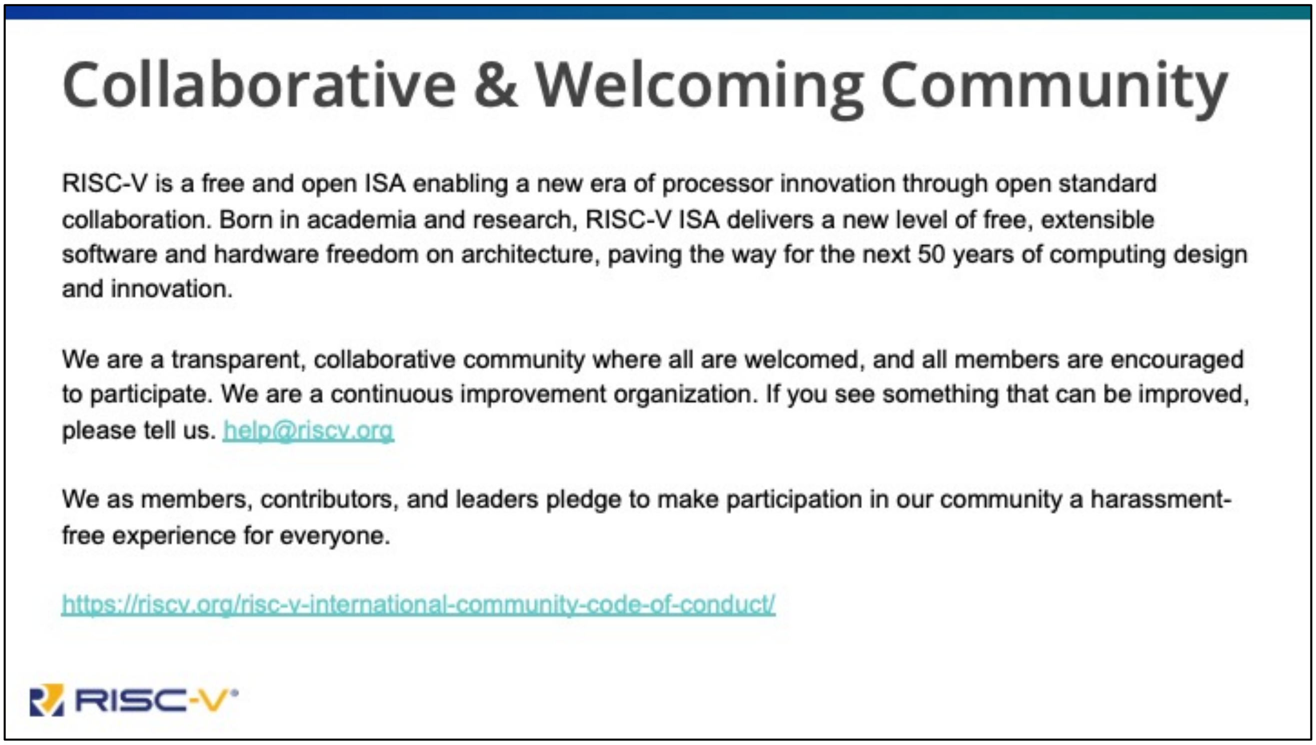


Antitrust Policy Notice

RISC-V International meetings involve participation by industry competitors, and it is the intention of RISC-V International to conduct all its activities in accordance with applicable antitrust and competition laws. It is therefore extremely important that attendees adhere to meeting agendas, and be aware of, and not participate in, any activities that are prohibited under applicable US state, federal or foreign antitrust and competition laws.

Examples of types of actions that are prohibited at RISC-V International meetings and in connection with RISC-V International activities are described in the RISC-V International Regulations Article 7 available here: https://riscv.org/regulations/

If you have questions about these matters, please contact your company counsel.



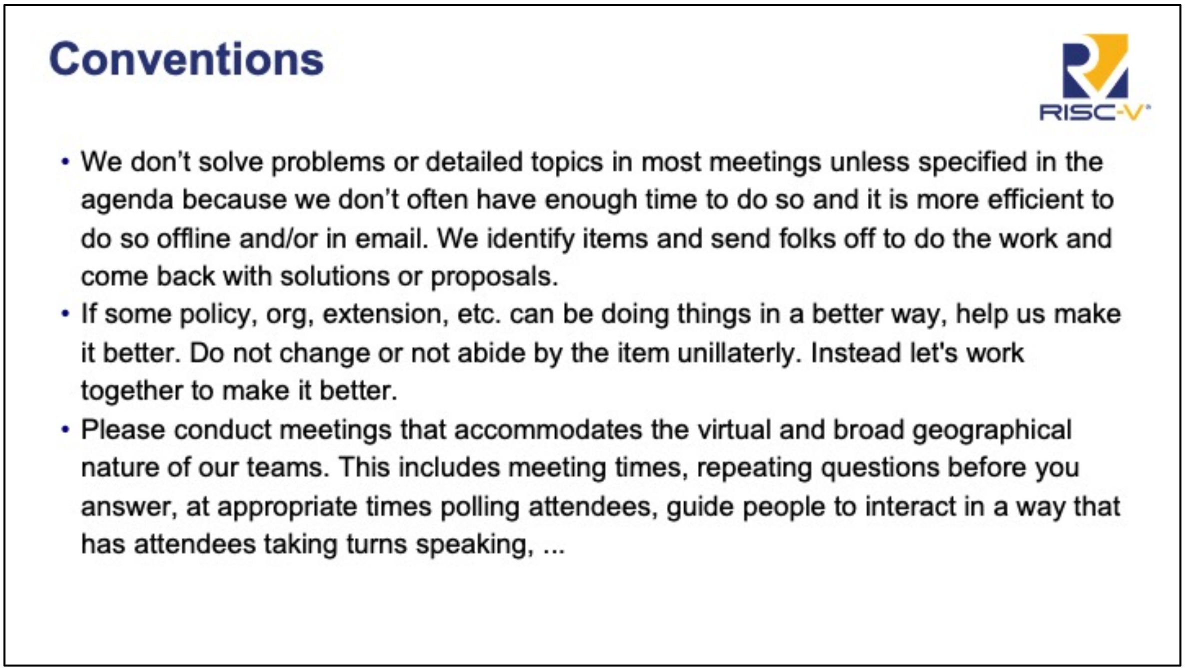
Collaborative & Welcoming Community

RISC-V is a free and open ISA enabling a new era of processor innovation through open standard collaboration. Born in academia and research, RISC-V ISA delivers a new level of free, extensible software and hardware freedom on architecture, paving the way for the next 50 years of computing design and innovation.

We are a transparent, collaborative community where all are welcomed, and all members are encouraged to participate. We are a continuous improvement organization. If you see something that can be improved, please tell us. help@riscv.org

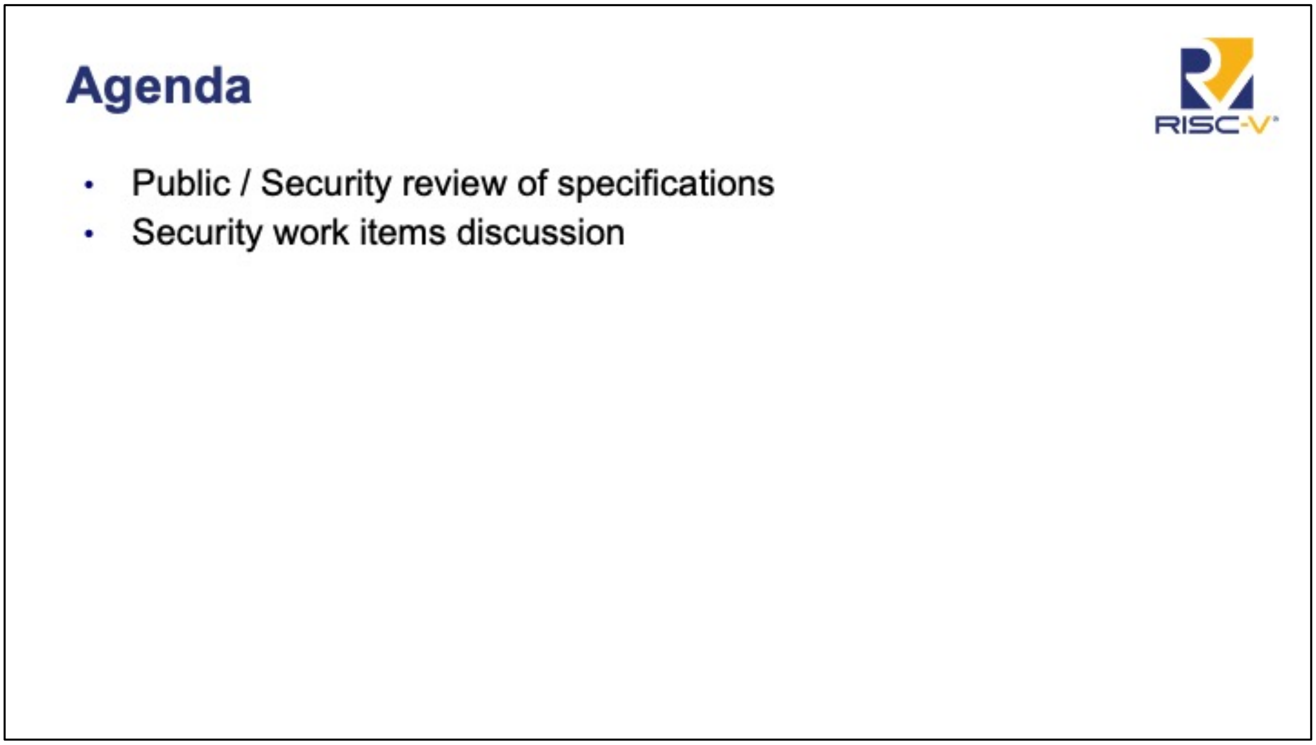
We as members, contributors, and leaders pledge to make participation in our community a harassment-free experience for everyone.

https://riscv.org/risc-v-international-community-code-of-conduct/



Conventions

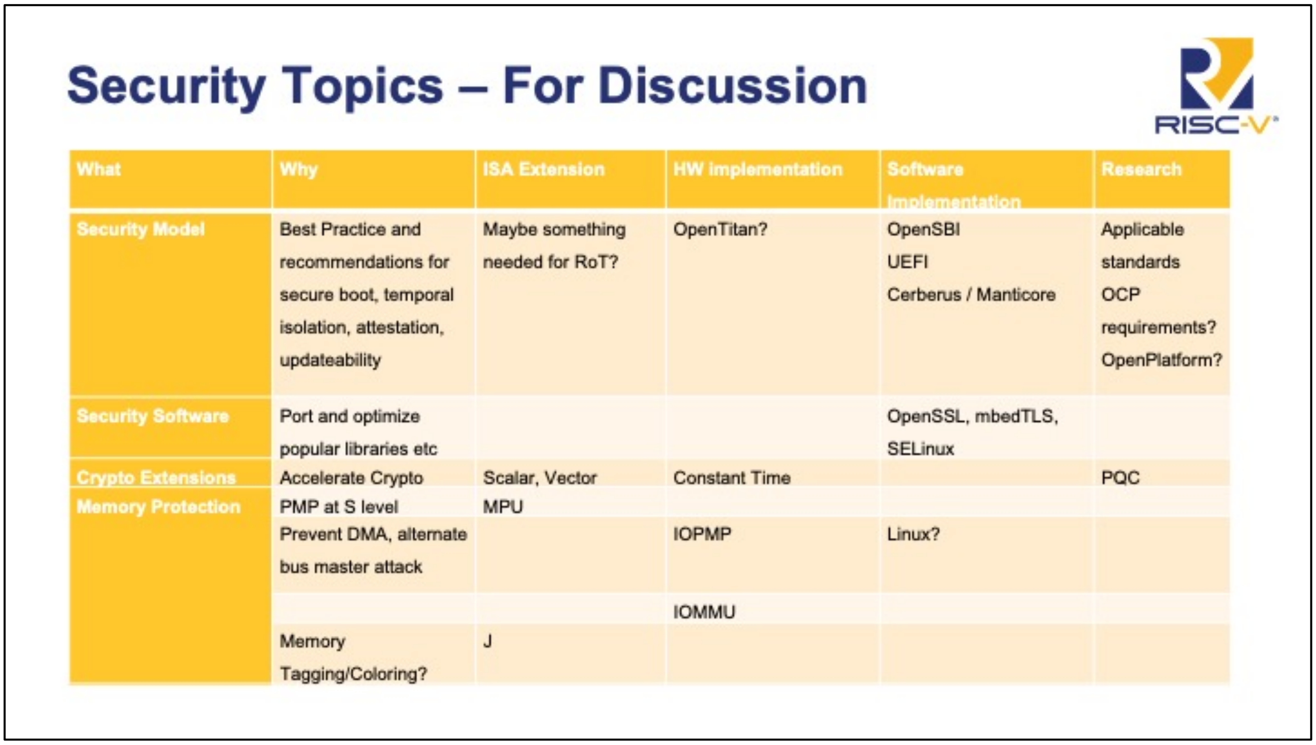
- We don’t solve problems or detailed topics in most meetings unless specified in the agenda because we don’t often have enough time to do so and it is more efficient to do so offline and/or in email. We identify items and send folks off to do the work and come back with solutions or proposals.
- If some policy, org, extension, etc. can be doing things in a better way, help us make it better. Do not change or not abide by the item unillaterly. Instead let's work together to make it better.
- Please conduct meetings that accommodates the virtual and broad geographical nature of our teams. This includes meeting times, repeating questions before you answer, at appropriate times polling attendees, guide people to interact in a way that has attendees taking turns speaking, ...



Agenda

- Public / Security review of specifications
- Security work items discussion

- There are currently 11 specifications going to Public Review that require a security review within next 45 days.



Security Topics – For Discussion

What	Why	ISA Extension	HW implementation	Software Implementation	Research
Security Model	Best Practice and recommendations for secure boot, temporal isolation, attestation, updateability	Maybe something needed for RoT?	OpenTitan?	OpenSBI UEFI Cerberus / Manticore	Applicable standards OCP requirements? OpenPlatform?
Security Software	Port and optimize popular libraries etc			OpenSSL, mbedTLS, SELinux	
Crypto Extensions	Accelerate Crypto	Scalar, Vector	Constant Time		PQC
Memory Protection	PMP at S level	MPU			
	Prevent DMA, alternate bus master attack		IOPMP	Linux?	
			IOMMU		
	Memory Tagging/Coloring?	J			

- Suresh volunteered to start work on Security Model

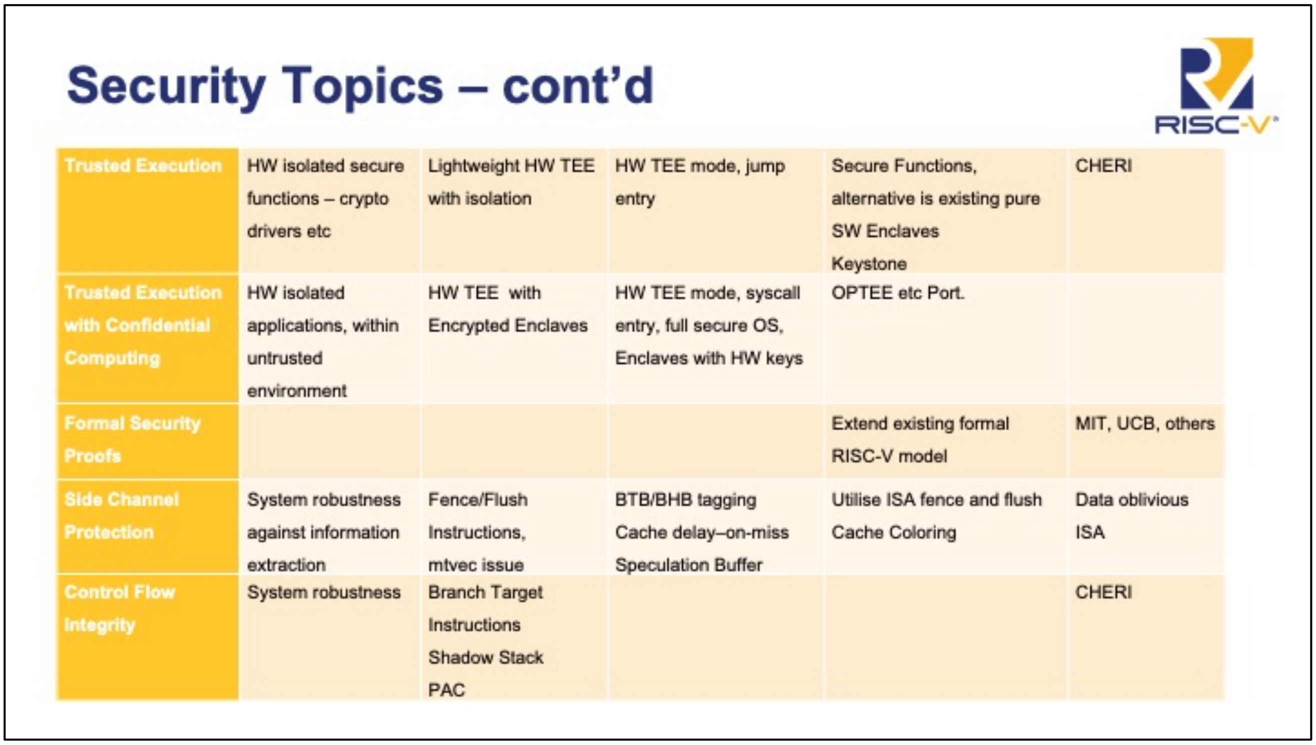
- Need for attestation, will need to distinguish between software guidance and hardware capabilities. Requires a (secure) Discovery mechanism at ISA level, already in discussion within RISC-V.

AI: Manuel/Andy confirm that Discovery is actively worked.

- PQC: likely continued in Crypto TG under Richard.

AI: Manuel/ Andy to confirm with Richard

- Memory Protection topics/work under SIG chaired by Nick



Security Topics – cont’d

Trusted Execution	HW isolated secure functions – crypto drivers etc	Lightweight HW TEE with isolation	HW TEE mode, jump entry	Secure Functions, alternative is existing pure SW Enclaves Keystone	CHERI
Trusted Execution with Confidential Computing	HW isolated applications, within untrusted environment	HW TEE with Encrypted Enclaves	HW TEE mode, syscall entry, full secure OS, Enclaves with HW keys	OPTEE etc Port.	
Formal Security Proofs				Extend existing formal RISC-V model	MIT, UCB, others
Side Channel Protection	System robustness against information extraction	Fence/Flush Instructions, mtvec issue	BTB/BHB tagging Cache delay–on-miss Speculation Buffer	Utilise ISA fence and flush Cache Coloring	Data oblivious ISA
Control Flow Integrity	System robustness	Branch Target Instructions Shadow Stack PAC			CHERI

- TEE & Confidential Compute topics/work under SIG chaired by Suresh

AI: Manuel to send Suresh pointer to Keystone

- Side Channel:
  - requires scope discussion, e.g., does it include analogue. Looking for someone to lead/chair the discussion
  - There is an existing fence.t proposal Andy Glew

AI: Andy / Manuel to reach out to Andy to discuss status and next steps

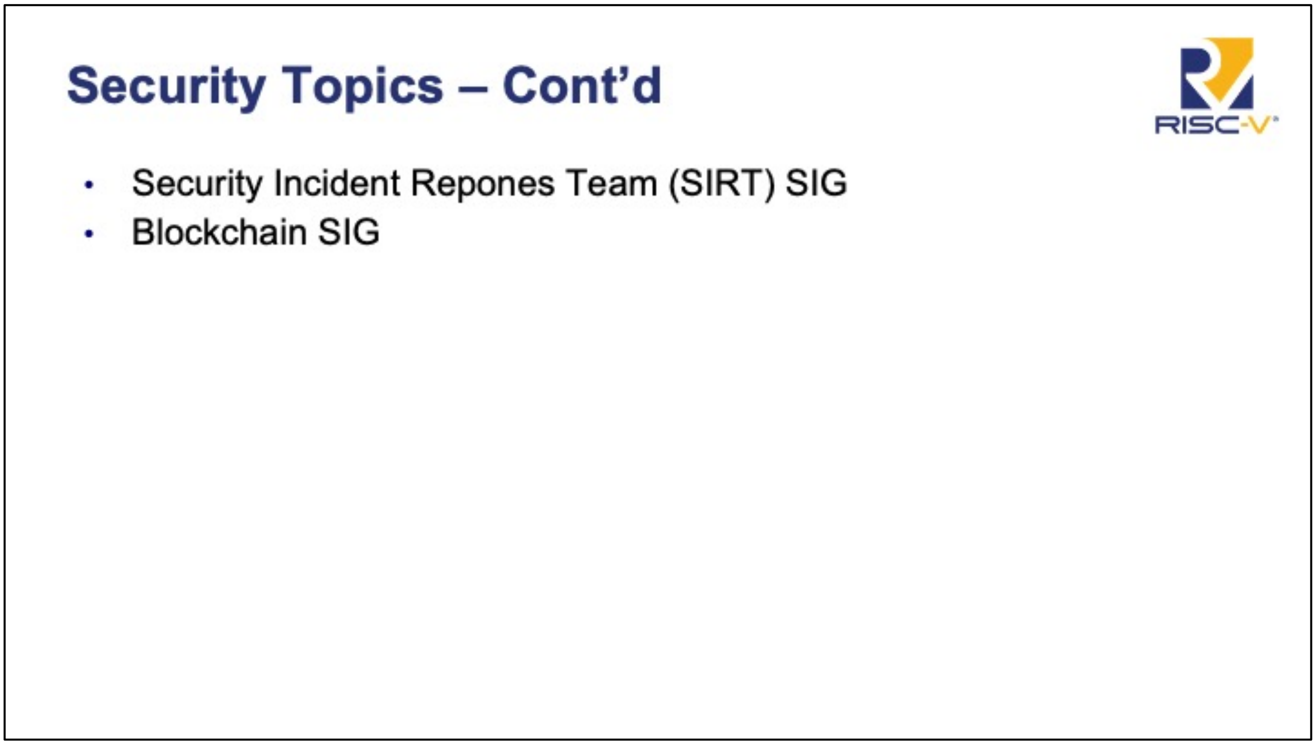
AI: Suresh may know potential candidate to lead Side Channel discussion, he will reach out to his contact at University of Illinois

- CFI: existing proposal, needs charter

AI: Andy / Manuel to validate if charter work can be started.

- CHERI: likely needs JWG under OS license

AI: Manuel / Jeff to verify if this fits within RISC-V legal framework



Security Topics – Cont’d

- Security Incident Repones Team (SIRT) SIG
- Blockchain SIG

- SIRT SIG in-process of updating riscv.org with responsible security disclosure information

- Functional Safety SIG: Andy assigned as liaison

Thank You

RISC-V