First Day

8:30 - 9:00 Welcome

9:00 - 9:45 Keynote 1: Ben Brown (ASCR/DOE) – IRI (In Person)

9:45 - 11:20

HPC Security Posture and Experience I

- Rob Gillen, ORNL, Industrial Strength Testbeds for HPC
- Matt Williams, Bristol University Title: “A greenfield AI supercomputing site's experience of implementing NIST SP 800-223” [Remote]
- Miguel Gila, CSCS [remote] Topic: security aspects on multi-tenancy environments
- Lovell-Troy, Alex Joseph, LANL, Cloud-like Security for on-prem HPC
- Derek Simmel (PSC) – NSF ACCESS Operations Cybersecurity

11:20 - 11:35 Break

11:35 - 12:05 Panel

Panel: Multi-tenant HPC Security (Panelist: Kevin McIver, David Wagenheim, Kathy Shonaiya, Spencer Shimko (SealingTech), Doug Johnson (OSC), Miguel Gila (CSCS))

12:05 - 1 pm Lunch

1:00 - 1:45
Keynote 2: Rachana Ananthakrishnan - Globus Auth: security fabric for distributed data and compute management

1:45 - 2:00 Break

2:00 - 3:40

HPC Data Security and Trusted HPC Environments

- Scott Russell (Indiana Univ) - Trusted CI [remote]
- Dr Christian Cole, University of Dundee, UK, “SATRE: Standardized Architecture for Trusted Research Environments” [Remote]
- Kyle Earley, Ohio Supercomputer Center, Secure Enclave for Protected Data Service

- Ryan Duitman (U Arizona), Data security compliance, also a panelist for data security in HPC)
- Hakizumwami Birali Runesha (UChicago)

3:40 - 5:00 Breakout session

Breakout Sessions [Kyle Earley, …]

- HPC Security Implementations, best practices, and challenges
    - Security implication in end-to-end scientific workflow
- Navigating security compliance requirements in HPC environments
- Future HPC system and its implications for security

Second Day

9:00-9:45 Keynote 3: Anita Nikolich (NCSA)

10:00 - 11:40 am

HPC Security Posture and Experience II

- Security Technical Exchange (Ian Lee)
- Lowell Wofford (AWS), AWS Approaches to zero trust for HPC+AI/ML
- Eric Eilertson (Microsoft): Encryption for HPC Networks Without Impacting Performance
- Ryan Adamson (ORNL) –Towards scalable fuzzing of an HPC Linux Kernel
- Phuong Cao (NCSA), PQC migration case study and risk assessments
- Vinu Joseph (NVIDIA Research), Accelerated Encrypted Computing using GPUs [remote]

11:40 am - 1:00 Lunch

1:00 - 1:45

Keynote 4: (NSF) – NAIRR Pilot [Katie Antypas]

1:45 - 2:00 break

2:00-3:30

RMF Development, Implementation, and Assessment and HPC Security Research

- Vicky Pillitteri (NIST) on CUI NIST 800-171
- Erik Deumens (UF), “Some options to implement RMF for research and development HPC systems”
- HPC Security Overlay NIST 800-234
- Yuede Ji (UT Arlington) – HPC containers security

3:30 - 4:00

Breakout Readout