First Day

8:30 - 9:00 **Welcome**

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

9:45 - 11:20 **HPC Security Posture and Experience I**

- Rob Gillen (Oak Ridge National Lab), *Industrial Strength Testbeds for HPC*
- Matt Williams (Bristol University, UK), *A greenfield AI supercomputing site's experience of implementing NIST SP 800-223* [Remote]
- Miguel Gila, CSCS (Swiss National Supercomputing Centre), *Security aspects on multi-tenancy environments* [Remote]
- Lovell-Troy, Alex Joseph (Los Alamos National Lab), *Cloud-like Security for on-prem HPC*
- Derek Simmel (Pittsburgh Supercomputing Center), *NSF ACCESS Operations Cybersecurity*

11:20 - 11:35 **Break**

11:35 - 12:05 **Panel: Multi-tenant HPC Security**

Moderator: Lowell Wofford (AWS)

Panelist: Miguel Gila (CSCS), Doug Johnson (OSC), Kevin McIver (Corvidtec), Spencer Shimko (SealingTech), Lowell Wofford (AWS)

12:05 - 1 pm **Lunch**

1:00 - 1:45 **Keynote 2: Rachana Ananthakrishnan - Globus: A Research IT Platform for Secure, Distributed Data and Compute Management**

1:45 - 2:00 **Break**

2:00 - 3:30 **HPC Data Security and Trusted HPC Environments**

- *Session Chair:* Hakizumwami Birali Runesha (UChicago)
- 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*
- Hakizumwami Birali Runesha (UChicago), *NIST Controls in HPC: Lessons in Implementation, Governance, Compliance, and Accelerated Time to Science*

3:30 - 4:00 **Panel: Supporting Data Security Compliance in an HPC environment**

Moderator: Birali Runesha (UChicago)

Panelist: Christian Cole (University of Dundee, UK), Ryan Duitman (U Arizona), Kyle Earley (Ohio Supercomputer Center), Scott Russell (Indiana Univ)

4:00 - 5:00 **Breakout session** [Kyle Earley, …]

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

Second Day

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

10:00 - 12:00 **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 (Oak Ridge National Lab), *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]

12:00 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), CUI NIST 800-171
- Erik Deumens (UF), *Some options to implement RMF for research and development HPC systems*
- Yuede Ji (UT Arlington), *HPC containers security*
- Yang Guo (NIST), *HPC Security Overlay NIST 800-234*

3:30 - 4:00 **Breakout Readout and Wrap up**