First Day: May 7, 2025 (Wednesday)

All times are in Eastern Daylight Time (EDT)

8:45 - 9:00 **Welcome: James St. Pierre (NIST)**

9:00 - 9:45 **Keynote 1: Ben Brown (ASCR/DOE) – HPC Security in an Integrated Future: A Perspective from DOE ASCR**

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

- *Session chair:* Puri Bangalore
- 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 In A Multi-tenant HPC Environment* [Remote]
- Alex Lovell-Troy (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) [remote], Doug Johnson (OSC), Kevin McIver (Corvidtec) [remote], Spencer Shimko (SealingTech) [remote], Lowell Wofford (AWS)

12:05 - 1 pm **Lunch**

1:00 - 1:45 **Keynote 2: Rachana Ananthakrishnan (UChicago) - 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), An Introduction to the Trusted CI Framework [remote]
- Dr Christian Cole (University of Dundee, UK), *A UK Specification for Trusted Research Environments* [Remote]
- Kyle Earley (Ohio Supercomputer Center), *OSC Secure Enclave: A roadmap towards NIST 800-171 compliance*
- Ryan Duitman (Univ of Arizona), *Journey to CUI HPC*
- 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) [remote], Ryan Duitman (U Arizona), Kyle Earley (Ohio Supercomputer Center), Scott Russell (Indiana Univ) [remote]

4:00 - 5:00 **Breakout session**

Breakout session chairs: Erik Deumens, Kyle Earley, Ian Lee, Yuede Ji, Albert Reuther, Hugo Hernandez

Note: there is one in-person session and one virtual session for each topic.

1. HPC Security Implementations, best practices, and challenges (Deumens, Hernandez)
    - Security implications in end-to-end scientific workflow
2. Navigating security compliance requirements in HPC environments (Earley, Lee)
3. Future HPC systems and their implications for security (Yuede Ji, Albert Reuther)

Second Day: May 8, 2025 (Thursday)

9:00-9:45 **Keynote 3: Anita Nikolich (NCSA): Trust & Verify: AI Security for Science**

10:00 - 11:30 **HPC Security Posture and Experience II**

- *Session Chair:* Ryan Adamson (ORNL)

- Ian Lee (ShorePoint, Inc.), Overview and lessons learned from HPC Security Technical Exchange
- 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*
- Vinu Joseph (NVIDIA Research), *Accelerated Encrypted Computing using GPUs* [Remote]

11:30 - 12:00 **Panel: Future of HPC Security**

Moderator: Ryan Adamson (ORNL)

Panelist: Ian Lee, Lowell Wofford, Eric Eilertson, Vinu Joseph [remote]

12:00 - 1:00 **Lunch**

1:00 - 1:45

Keynote 4: Katie Antypas (NSF): Accelerating AI Innovation and Workforce Development through the NAIRR Pilot [remote]

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

2:00-3:30 **RMF Development, Implementation, and Assessment and HPC Security Research**

- *Session chair:* Erik Deumens (UF)
- Vicky Pillitteri (NIST), *Overview of the NIST Protecting CUI Series: NIST SP 800-171r3, SP 800-171Ar3, SP 800-172r3 & SP 800-172A*
- Erik Deumens (UF), *Some options to Implement RMF for Research and Development HPC Systems*
- Yuede Ji (UT Arlington), *HPC Containers Security*
- Phuong Cao (NCSA), *PQC Migration Case Study and Risk Assessments* [Remote]
- Yang Guo (NIST), *HPC Security Overlay NIST 800-234*

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