

First Day: July 22, 2026 (Wednesday)

All times are in Eastern Daylight Time (EDT)

9:00 – 9:15 **Welcome Speech: Kevin Stine (NIST/ITL)**

9:15 – 9:30 **Opening Remarks: Saleela Khanum Salahuddin (ODNI)**

9:30 – 10:15 **Keynote 1: Ed Walker (NSF/OAC), *Supporting Trustworthy Scientific Discovery and Innovation on our Nation's Scientific Cyberinfrastructure***

10:15 – 10:25 **Break**

10:25 – 12:05 **AI Data Center Architecture, Component, and Workload**

Session chair: Yang Guo (ITL)

- Alex Dent (Qualcomm), *Confidential Computation with PIM Memory*
- Amy Chang (Cisco), *Powering the Agentic Era: The Importance of Resilient Data Centers for the Future of AI*
- Lowell Wofford (AWS), *Can AI live in the Walled Garden? Comparing HPC and AI Security Patterns*
- Luca Maria Castiglione and Isaac Matthews (HPE): *Securing AI Workloads with Trusted Execution Environments and Multi-Party Attestation*

12:05 – 1:00 pm **Lunch Break**

1:00 – 3:05 **AI Data Center Security, Standards, and Guidelines**

Session chair: Martin Stanley (ITL)

- Lisa Thiergart (SL5 Task Force), *Security Level 5 - a new Overlay for Nation-State Secure Frontier AI Datacenters*
- Jair Aguirre (RAND), *RAND SL3 Standard*
- Erich Devendorf (RAND), *Integrity First: Receipts Not Vibes*
- Bennett Tomlinson (CAISI), *AI Data Center Security Standard Framework*
- Yang Guo (ITL), *AI Data Center Computing Environment Security Analysis: A High-Performance Computing (HPC) Driven Approach*

3:05 – 3:15 **Break**

3:15 – 4:30 **Breakout session**

1. **Computing infrastructure security:** AI data center computing infrastructure security implementations, best practices, and challenges
Session chairs: Lowell Wofford (AWS), Noah Pavuk (ORNL)
2. **Facilities security:** AI data center Operational Technology (OT), facility construction, power and sustainability, and physical and personnel security
Session chairs: Rickey Gregg (DoW/HPCMP), Jennifer Allphin (DoW/HPCMP)
3. **Standards and guidelines:** AI data center security standards and guidelines, regulatory and compliance challenges
Session chairs: Erik Deumens (University of Florida), John Williams (DoW/HPCMP)
4. **Supply chain security:** AI data center supply chain
Session chairs: Rebecca McWhite (NIST), Siva Ilagovan (Tech Mahindra)

Second Day: July 23, 2026 (Thursday)

9:30 – 10:15 **Keynote 2: Ben Brown (DoE/ASCR), *An Update from the Genesis Mission: Building the Genesis Platform Minimum Viable Product***

10:15 – 10:30 **Break**

10:30 – 11:45 **AI Data Center AI Security, Access control, Monitoring, and Operation (I)**

Session chair: Rickey Gregg (DoW/HPCMP)

- Marcus Fitts (SMET.ai), *Converged Security Operations for Frontier AI Data Centers*
- Noah Pavuk (ORNL), *Providing and Securing institutional AI services in HPC*
- Elizabeth Guillot (CrowdStrike), *Securing the AI Tech Stack*

11:45 – 1:00 **Lunch Break**

1:00 – 2:15 **AI Data Center AI Security, Access control, Monitoring, and Operation (II)**

Session chair: Sanjay (Jay) Rekhi (ITL)

- Erik Deumens (University of Florida), *AI services infrastructure: from data center to chat prompt*
- Tom Green (University of Bristol, UK), *Adopting the NCSC Cybersecurity Assessment Framework for a leadership class AI supercomputer*
- Siva Ilagovan (Tech Mahindra): *Mythos Readiness: CISO AI Modern Defense Strategies*

2:15 – 2:25 **Break**

2:25 – 4:05 AI Data Center Secure OT, Construction, and Physical Security

Session chair: Bennett Tomlinson (CAISI)

- Grant Bartlett (SMET.ai), *Securing the Substrate: A defense-in-depth framework for nation-state, corporate, and civil threat resilience across the compute and MEP systems of frontier AI facilities*
- Ashley Hedrick (SMET.ai), *AI Data Centers — Structural Gaps Between Legacy Practice and AI Infrastructure*
- Soumyendu Sarkar (HPE), *When AI Manages the AI Data Center: Secure Agentic Autonomy for Compute, Liquid Cooling, and Energy Co-Optimization*
- Luis Cosio (SL5), *AI705 - Overlay on ICD705 for Nation-State Secure Work Areas and Emanation Protection for Frontier AI Datacenters*

4:05 – 4:30 Readout and Wrap up

Session chair: Yang Guo and Bennett Tomlinson (NIST)