Panel on Review of Selected Divisions of the
National Institute of Standards and Technology (NIST)
Information Technology Laboratory (ITL)
June 4-6, 2024

SUB-PANEL AGENDA
COMPUTER SECURITY DIVISION
(All times are EDT)

Tuesday, June 4, 2024

For activities before 11:00 a.m., please see the master agenda.

Location: All sessions in National Cybersecurity Center of Excellence Room 3
DATA GATHERING SESSIONS (OPEN TO THE PUBLIC)

11:00 a.m. – 1:00 p.m.	**Division and Group Overviews**, multiple presenters *Includes working lunch with division leadership.*
1:00 – 2:15 p.m.	**Combinatorial Methods in Software Assurance**, Rick Kuhn, *Security Components and Mechanisms Group, ITL* **Next-Generation Access Control**, David Ferraiolo*, Secure Systems and Applications Group, ITL*
2:15 – 2:30 p.m.	*Break*
2:30 – 4:00 p.m.	**Block Cypher Modes of Operations**, Morris Dworkin, *Cryptographic Technology Group, ITL* **Diaoptra: A Test Platform for AI Models**, Harold Booth, *Security Components and Mechanisms Group, ITL*
4:00 – 4:15 p.m.	*Break*
4:15 – 5:00 p.m.	**Post-Quantum Cryptography**, Dustin Moody, *Cryptographic Technology Group, ITL*

For activities after 5:00 p.m., please see the master agenda.

Wednesday, June 5, 2024

Location: All sessions in NIST Gaithersburg Campus, Building 101, Lecture Room B
DATA GATHERING SESSIONS (OPEN TO THE PUBLIC)

10:00 a.m. – 12:00 noon	**Protecting Controlled Unclassified Information Security**, Victoria Pillitteri, *Security Engineering and Risk Management Group, ITL* **National Vulnerability Database**, Tanya Brewer, *Security Test, Validation and Measurement Group, ITL*

	Crypto Module Validation Program, Dave Hawes, *Security Test, Validation and Measurement Group, ITL*
12:00 noon – 1:00 p.m.	**Working Lunch with Postdocs and Early Career Staff**
1:00 – 2:15 p.m.	**Lightweight Cryptography**, Meltem Sonmez Turan and Kerry McKay, *Cryptographic Technology Group, ITL*
	Hardware Security, Sanjay (Jay) Rekhi, *Security Components and Mechanisms Group, ITL*
2:15 – 2:30 p.m.	*Break*
2:30 – 4:00 p.m.	**Security Guidance for Microservices-based Application Architectures**, Ramaswamy (Mouli) Chandramouli, *Secure Systems and Applications Group, ITL*
	Risk Management Framework, Cybersecurity Supply Chain Risk Management and the SP 800-53 Security and Privacy Controls, Victoria Pillitteri and Derek Sappington, *Security Engineering and Risk Management Group, ITL*; Rebecca McWhite, *Computer Security Division, ITL*

For activities after 4:00 p.m., please see the master agenda.