NIST IoT Cybersecurity Colloquium – Draft Agenda

Tue, Mar 31 – Wed, Apr 1, 2026 | Gaithersburg, MD

Objective: This workshop is intended to provide stakeholders an update on the NIST Cybersecurity for IoT Program, as well asl to collect\ inputs on selected topics to understand priorities for updating SP 800-213 and creation of future guidance.

Draft Agenda

Day 1 | Tue, Mar 31, 2026

Time	Topic	Proposed Speakers
9:00-9:30	Speaker: Welcome & Opening Remarks	Mike Fagan (NIST)
9:30-9:45	Speaker: NIST IoT Cyber & Dept of Commerce priorities	Kat Megas (NIST)
9:45-10:00	Speaker: Setting the Stage	Mike Fagan (NIST)
10:00-10:45	Presentation: Identity of Things	Nick Allott (Nquiring Minds)
10:45-11:00	Break	
11:00-12:00	Fireside Chat: Discussion of Light-weight Cryptography, Post Quantum Cryptography and IoT	TBD
12:00-1:30	Lunch	
1:30–3:30	Breakout Sessions: SP 800-213 – Discussion of Revision 1 Topics	

Day 2 | Wed, Apr 1, 2026

Time	Topic	Speakers
9:00-9:30	Speaker: Welcome & Focus on the Future / Overview Day 1's NIST SP 800-213 Breakouts	Mike Fagan (NIST)
9:30-10:30	*Keynoter:* ***The Evolution of IoT in the Age of AI: How AI-Native Systems Redefine Cybersecurity and Trust***	Benson Chan (Strategy of Things)
10:30-11:45	Panel: Healthcare Considerations – Real world application and IoT Cybersecurity controls	Jeff Marron (NIST) (moderator)
11:45-1	Lunch	
1:00-2:00	Panel: IoT Risk In Context	TBD

DRAFT

2:00-3:30	Breakout Session: IoT Risk Considerations	
3:30-3:45	Wrap-up & Conclusion	Mike Fagan (NIST)

Please link the following Abstract to Benson Chan's keynote on Day 2

The Evolution of IoT in the Age of AI: How AI-Native Systems Redefine Cybersecurity and Trust

The Internet of Things (IoT) is evolving from connected devices and sensor networks that monitor the physical environment into systems where intelligence is embedded directly into operations. Emerging capabilities in generative and agentic AI signal a shift toward environments where AI-enabled systems do more than detect and predict anomalies. These systems can diagnose conditions, recommend responses, and increasingly coordinate or execute actions across physical and digital domains. Together, these developments are pushing IoT toward operating models in which AI plays an active role in how systems function and decisions are made.

Future IoT environments will be AI-native, designed from the outset with artificial intelligence as an integral part of system operations rather than a separate decision-support or analytics function. As IoT progresses toward AI-enabled and more autonomous, outcome-driven systems, the scope of cybersecurity expands beyond protecting devices, networks, and data. Cybersecurity and privacy remain essential, but they become components of a broader challenge: establishing and maintaining trust in system behavior. This includes assuring data integrity, model reliability, decision transparency, operational resilience, and effective human governance. This keynote offers a forward-looking perspective on how standards, risk frameworks, and assurance practices must evolve from securing infrastructure to enabling justified trust in intelligent, adaptive systems.

DRAFT