THE VITALS:
STANDARDS ACTIVITIES OF NIST'S IT LAB

The United States' global technological leadership relies on unwavering strength in standards development. Our robust engagement in standards for critical and emerging technologies is strengthening U.S. economic competitiveness now and for years to come.

CONNECTED TO NIST | CRITICAL & EMERGING TECHNOLOGY (CET) AREAS

Several critical and emerging technologies have strong relevance to NIST and NIST'S Information Technology Lab (ITL), specifically.

Example Critical & Emerging Technologies	Relevant NIST/ITL Projects, Programs & Efforts
Communication & Networking Technology	5G Cybersecurity
Semiconductors & Microelectronics	Hardware Security
AI & Machine Learning	AI AI Safety Institute
Digital Identity Infrastructure & Distributed Ledger Technologies	Identity & Access Management Blockchain
Quantum Information Technology	PQC standardization
Automated & Connected Infrastructure	Cybersecurity for IoT
Automated, Connected & Electrified Transportation	EV Cybersecurity Automotive Cybersecurity Community of Interest
Cybersecurity & Privacy	Cybersecurity & Privacy

STANDARDS BODIES

ITL's research underpins our contributions to standards bodies. Our staff engages in many CET-related standards activities that include:

- **Advancing 5G network security** by participating in 3GPP's SA3 working group that is modernizing the cryptographic protocols used in 5G networks.
- **Progressing standardization activities related to identity and access management**, including through contributions to parts of the ISO/IEC 18013 standard regarding mobile driving licenses, strong engagement in the World Wide Web Consortium's Federated Credential Management Community Group, and participation across multiple working groups within the Open ID Foundation and the FIDO Alliance.
- **Holding leadership roles in ISO TC 307's blockchain and distributed ledger technologies work** and its US mirror committee by playing an instrumental role in launching a US-led project on Physical Assets disposition, ISO/AWI 20435.
- **Facilitating alignment between NIST guidance on post-quantum cryptography and international standards,** including through contributions ISO/IEC14888-4 on stateful hash-based signatures. NIST staff have served as co-editor on ISO/IEC PWI 19541 regarding key encapsulation mechanisms for Post-Quantum Cryptography.
- **Advancing standardization of Internet of Things (IoT) security** through active participation in ISO/IEC JTC 1/SC 41 activities and significant

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

contributions to ISO/IEC 27404 and ISO/IEC 27402. Within IETF, NIST co-chaired the Software Updates for Internet of Things (SUIT) working group focused on designing a firmware update solution suitable for tiny IoT devices.

- **Leading cyber infrastructure standardization activities,** including by serving as Vice Chair of the INCITS Steering Committee for ISO/IEC JTC 1 SC 38, the WG 3 Ad-Hoc Chair within SC 38, the SC 38 Advisory Group Stakeholder Engagement Chair, and serving as Head of Delegation for the Spring 2023 SC 38 plenary meetings. NIST served as Chair of the Industry IoT (II) Consortium Architecture and Patterns Task Group and various draft standards within the II Consortium. NIST also participates in the ISA99 committee which authors the standards and leads the joint team which is looking at industrial internet of things and industrial cloud services.

- **Leading the U.S. technical advisory group focused on automotive cybersecurity standardization** (ISO/IEC TC 22) and contributing to the publication of the first international standard on updates to vehicles, ISO 24089:2023. NIST staff served as the co-chair for the Cybersecurity Assurance Levels/Targeted Attack Feasibility project group that is implementing follow-up work to this first of its kind international standard.

- **Holding leadership roles in AI standardization** including by chairing ISO/IEC JTC 1 SC 42 WG 2 on AI and Data. The efforts of WG 2 advanced and matured ISO/IEC 5259 - Parts 1-5. NIST is also contributing to ISO/IEC AWI 27090 on addressing the cybersecurity threats and failures in AI systems.

- **Facilitating alignment between NIST cybersecurity risk management guidance and international standards,** in particular alignment between the NIST Cybersecurity Framework 2.0 and ISO cybersecurity standards. NIST has also facilitated recent contributions to the National Online Informative References (OLIR) Program demonstrating the relationship between NIST cybersecurity guidance, regulations, and standards.

- **Advancing consumer trust in the digital economy** through extensive technical contributions to ISO/IEC 31700 and ISO/IEC 27557, which offers a framework for assessing organizational privacy risk including privacy impacts on individuals.

WANT TO LEARN MORE?

- **VISIT OUR WEBSITE**

- **LEARN MORE ABOUT NIST'S ROLE IN STANDARDS DEVELOPMENT**