



# National IoT Security Roadmap

## (Draft)



Vision	2024	2025	2026	2027	2028	2029	2030	2031	2032	2033	2034	2035	2036	2037	2038	2039	2040	2041	2042	2043	2044	2045	2046	2047
IoT DEVICE SECURITY	IoT Sand box – Functional Security and Validation																							
	Authentication, Access Control and Data Handling of IoT Devices																							
	Sensors and Actuators																							
	IoT Device Certificate Lifecycle Management (PKI for IoT Devices, Certification Revocation, etc.)																							
IoT NETWORK SECURITY	IoT Network Security Orchestration and Automation (Threat Modeling, Automate Trust Management and Security Configuration, etc. )																							
	Satellite Connectivity																							
	eSIM																							
	Zero Trust Architecture																							
IoT APPLICATION SECURITY	IoT Protocols (CoAP, MQTT, etc.) Security										Self-aware IoT Protocols and its Security													
	VAPT and Threat Analysis																							
	oneM2M																							
IoT CLOUD PLATFORM SECURITY	Secure Data Center Management (Cloud)																							
AI BASED IoT SECURITY	AI Enabled Botnet Detection and DNS Ecosystem																							
	AI Enabled Privacy and Data Protection																							
	Artificial Intelligence of Things (AIoT)																							
QUANTUM ENABLED IoT SECURITY	Low power & Lightweight PQC																							
	Secure IoT Network through QKD and SDN																							
LIGHTWEIGHT CRYPTOGRAPHY	Low-power Quantum Random Number Generators (QRNG)										Low power to No power Cryptography algorithms for IoT													
	Blockchain assisted IoT Security																							
	Low footprint Cryptographic Algorithms (ASCON, etc.)																							
SEMICONDUCTORS IoT SECURITY	RISC-V based Secure SoC for IoT										Indigenous Chip Design and Standards													
STANDARDS AND GUIDELINES FOR IoT SECURITY	Collaborating with IoT Security Working Groups for Constant Updation of Policies																							
	IoT Security Guidelines Framework Formulation																							

Short Term    Medium Term    Long Term

### Goals

- Indigenous security ecosystem for IoT security
- AI powered self adapting IoT security
- PQC enabled IoT systems
- No power cryptography algorithms for IoT
- Security on IoT enabled Digital Twins

### Major Outcomes

- AI/ML/DL based IoT security solution
- Enhancement in IoT security and its evaluation strategies
- Secure SoC for IoT devices
- IoT Security with low power and lightweight cryptography algorithms
- IoT Security fortified with PQC
- IoT device certification

### Beneficiaries

- Enterprises and Businesses
- Consumers and IoT device Manufactures
- IoT S/W and H/W Developers
- Regulatory Bodies and Governments
- Research Community