AKWA IBOM STATE HOUSE OF ASSEMBLY

AKWA IBOM STATE EDGE COMPUTING AND CRITICAL IoT INFRASTRUCTURE SECURITY BILL, 2026

A BILL

FOR A LAW TO REGULATE EDGE COMPUTING SYSTEMS, INTERNET OF THINGS DEVICES, SMART METERS AND CRITICAL TELEMETRIC INFRASTRUCTURE DEPLOYED IN AKWA IBOM STATE; TO PROVIDE FOR CYBERSECURITY, DATA SECURITY, SUPPLY CHAIN SECURITY AND INCIDENT REPORTING AND FOR RELATED MATTERS

Sponsor: Hon. (Engr.) Uduak-Obong Ekpo-Ufot

Co-Sponsors:

Rt. Hon. Kufreabasi Edidem

Rt. Hon. (Barr.) Otobong Bob

Rt. Hon Asuquo Nana Udo

Rt.Hon. Mfon Idung

Hon. (Dr.) Nsidibe Akata

Hon. Sunday Johnny

Hon. Uwemedimo Asuquo

Hon. Eric Akpan

Hon. Uwem Imoh-Ita

Hon. Emem Udom

Arrangement of Sections

PART I

Preliminary Provisions

1. Objectives
2. Application and Regulatory Scope

PART II

Administration And Governance

3. Establishment of the State Edge and IoT Security Authority
4. Functions of the Authority

PART III

Critical IoT And Edge Infrastructure Security

5. Classification of Critical IoT Infrastructure
6. Minimum Hardware Security Standards
7. Secure-by-Design Requirement
8. Device Identity and Authentication
9. Encryption and Communications Security
10. Secure Firmware and Over-the-Air Updates
11. Hardware and Software Bill of Materials
12. Vulnerability Disclosure and Remediation
13. End-of-Life and End-of-Support Obligations

PART IV

Edge Computing And Data Localization

14. Establishment of Edge Data Localization Zones
15. Local Processing of Critical Telemetry
16. Data Minimisation and Anonymisation
17. Restrictions on Cross-Border Transfer and External Cloud Processing
18. Clearance for External Processing

PART V

Supply-Chain And Procurement Security

19. Security Requirements for Suppliers and Contractors
20. Security Due Diligence
21. Trusted Supplier Requirements
22. Prohibition of Defective or Non-Compliant Deployments
23. Procurement Debarment

PART VI

Security Testing, Monitoring And Incident Response

24. Security Assessment and Certification
25. Independent Security Audits
26. Cybersecurity Incident Reporting
27. Critical Incident Notification
28. Incident Response and Recovery
29. Emergency Security Measures

PART VII

Regulatory Sandbox And Innovation

30. Edge Computing and IoT Regulatory Sandbox
31. Research and Innovation Exemptions

PART VIII

Consumer, Public And Citizen Protection

32. Protection of Citizens and Public Services
33. Protection Against Unauthorised Device Manipulation

PART IX

Enforcement, Offences And Penalties

34. Compliance Notices
35. Administrative Sanctions

36. Offences and Penalties

37. Corporate Liability

38. Aggravating and Mitigating Factors

39. Restitution and Remediation

40. Appeals

PART X

Fees, Finance And Miscellaneous

41. Fees, Charges and Cost Recovery

42. Fund for Critical Digital Infrastructure Security

43. Regulations

44. Confidentiality and Protection of Security Information

45. Cooperation with Federal Authorities

46. Limitation of Liability

47. Transitional Provisions

48. Savings

49. Interpretation

50. Short Title

Schedule

A LAW TO REGULATE EDGE COMPUTING SYSTEMS, INTERNET OF THINGS DEVICES, SMART METERS AND CRITICAL TELEMETRIC INFRASTRUCTURE DEPLOYED IN AKWA IBOM STATE; TO PROVIDE FOR CYBERSECURITY, DATA SECURITY, SUPPLY CHAIN SECURITY AND INCIDENT REPORTING AND FOR RELATED MATTERS

BE IT ENACTED by the Akwa Ibom State House of Assembly as follows -

{Commencement: }

PART I

PRELIMINARY PROVISIONS

1. Objectives

The objectives of this Law are to—

(a) protect critical Internet of Things infrastructure deployed within Akwa Ibom State;

(b) establish minimum cybersecurity and hardware-security standards for IoT devices and edge computing systems;

(c) promote secure-by-design principles in public digital infrastructure;

(d) protect municipal utilities, smart grids, public transportation systems, healthcare infrastructure, water systems and other critical services against cyber threats;

(e) establish secure Edge Data Localization Zones within the State;

(f) promote secure local processing of critical public telemetry;

(g) strengthen cybersecurity throughout the technology supply chain;

(h) establish obligations for manufacturers, suppliers, contractors, operators and service providers;

(i) promote resilience and continuity of critical public services;

(j) encourage responsible deployment of edge computing and IoT technologies; and

(k) protect the digital sovereignty, economic interests and security of Akwa Ibom State while remaining consistent with applicable Federal law.

2. Application and Regulatory Scope

(1) This Law applies to critical IoT devices, smart meters, edge computing nodes, sensors, gateways, controllers, telemetry systems and associated networks deployed, operated or maintained—

(a) by the State Government;

(b) by a local government council;

(c) by a State-owned or State-controlled entity;

(d) by a public institution operating in the State;

(e) by a contractor providing services to the State; or

(f) in any other critical infrastructure designated under this Law.

(2) The Law may apply to private infrastructure where the infrastructure—

(a) provides a critical service to the public;

(b) is materially connected to State critical infrastructure; or

(c) is designated as critical infrastructure by regulations made under this Law.

PART II
ADMINISTRATION AND GOVERNANCE

3. Establishment of the State Edge and IoT Security Authority

There is established an Akwa Ibom State Edge and IoT Security Authority, which shall be responsible for coordinating the implementation of this Law.The Governor may designate an existing State digital innovation, ICT, cybersecurity or technology agency to perform the functions of the Authority.

4. Functions of the Authority

The Authority shall—

(a) develop minimum security standards for critical IoT infrastructure;

(b) maintain a register of critical IoT infrastructure;

(c) designate Edge Data Localization Zones;

(d) establish cybersecurity certification requirements;

(e) conduct or coordinate security assessments;

(f) monitor compliance;

(g) coordinate vulnerability disclosure;

(h) receive and coordinate incident reports;

(i) establish technical standards for edge computing;

(j) coordinate with relevant Federal authorities;

(k) promote research and innovation;

(l) operate or supervise an IoT regulatory sandbox; and

(m) perform such other functions as may be necessary to achieve the objectives of this Law.

PART III

CRITICAL IoT AND EDGE INFRASTRUCTURE SECURITY

5. Classification of Critical IoT Infrastructure

The Authority shall establish a risk-based classification system which may include—

(a) **Class I — Essential Infrastructure**

Systems whose disruption may threaten life, public safety or essential services.

(b) **Class II — Critical Public Infrastructure**

Systems supporting utilities, transportation, public administration or major economic infrastructure.

(c) **Class III — Significant Infrastructure**

Systems whose compromise may cause substantial operational or economic disruption.

6. Minimum Hardware Security Standards

All critical IoT devices and edge nodes deployed in State infrastructure shall—

(a) support secure authentication;

(b) implement appropriate encryption;

(c) support secure firmware updates;

(d) maintain tamper-resistant security mechanisms where appropriate;

(e) support secure logging;

(f) prevent the use of default administrative credentials;

(g) provide mechanisms for vulnerability remediation; and

(h) comply with standards prescribed by the Authority.

7. Secure-by-Design Requirement

A person shall not deploy critical IoT infrastructure unless reasonable security measures have been incorporated into the design, development, testing and deployment lifecycle. Security shall not be treated solely as an after-deployment measure.

8. Device Identity and Authentication

Critical IoT devices shall possess unique and verifiable identities and shall use appropriate authentication mechanisms for communication with authorised networks and systems.

Shared default credentials shall be prohibited.

9. Encryption and Communications Security

Critical IoT infrastructure shall employ appropriate encryption for—

(a) communications;

(b) authentication credentials;

(c) sensitive data stored on devices;

(d) communication between IoT devices and edge nodes; and

(e) communication between edge nodes and authorised cloud infrastructure.

10. Secure Firmware and Over-the-Air Updates

Manufacturers and suppliers of critical IoT devices shall—

(a) provide mechanisms for secure firmware updates;

(b) authenticate firmware before installation;

(c) prevent unauthorised modification;

(d) maintain security updates throughout the declared support period; and

(e) provide mechanisms for emergency security patches.

11. Hardware and Software Bill of Materials

A supplier of critical IoT equipment to the State shall provide, where prescribed by regulations—

(a) a Hardware Bill of Materials;

(b) a Software Bill of Materials;

(c) information relating to third-party components;

(d) known vulnerabilities;

(e) licensing information; and

(f) declared support and end-of-life dates.

12. Vulnerability Disclosure and Remediation

Manufacturers and suppliers shall maintain an appropriate vulnerability disclosure mechanism and shall—

(a) receive vulnerability reports;

(b) investigate reported vulnerabilities;

(c) notify affected operators of material vulnerabilities;

(d) provide remediation or mitigation within prescribed periods; and

(e) maintain records of material vulnerabilities.

13. End-of-Life and End-of-Support Obligations

A manufacturer or supplier shall disclose the expected security-support period of a critical IoT device before deployment.

An operator shall not deploy equipment for critical infrastructure where the manufacturer has discontinued security support, except where the Authority grants a temporary exemption subject to compensating security controls.

PART IV

EDGE COMPUTING AND DATA LOCALIZATION

14. Establishment of Edge Data Localization Zones

The Authority may designate secure physical or logical environments within the State as Edge Data Localization Zones for the processing, filtering, anonymisation or storage of critical public telemetry.

15. Local Processing of Critical Telemetry

Critical public telemetry generated within the State shall, where technically and economically practicable, be processed through an authorised Edge Data Localization Zone before being transmitted to external cloud infrastructure.

16. Data Minimisation and Anonymisation

Operators shall—

(a) collect only data reasonably necessary for the intended function;

(b) anonymise or pseudonymise data where practicable;

(c) avoid unnecessary transmission of raw data; and

(d) implement appropriate retention and deletion controls.

17. Restrictions on External Cloud Processing

Raw, unencrypted or otherwise sensitive critical infrastructure data shall not be transferred to an external cloud environment outside Nigeria except in accordance with—

(a) applicable Federal law;

(b) applicable data protection requirements; and

(c) a clearance or authorisation issued under this Law where such clearance is required.

18. Clearance for External Processing

The Authority may establish a clearance mechanism for the external processing of specified categories of critical infrastructure data.

The Authority shall consider—

(a) cybersecurity risk;

(b) jurisdiction of the receiving service provider;

(c) encryption;

(d) data sensitivity;

(e) business continuity;

(f) national and State security considerations; and

(g) applicable Federal requirements.

PART V
SUPPLY-CHAIN AND PROCUREMENT SECURITY

19. Security Requirements for Suppliers and Contractors

Every contractor supplying critical IoT infrastructure to the State shall comply with prescribed cybersecurity requirements.

20. Security Due Diligence

Before procurement, the relevant State institution shall undertake reasonable due diligence regarding—

(a) manufacturer;

(b) software components;

(c) country and supply chain of origin;

(d) vulnerability history;

(e) security-support commitments;

(f) ownership and control; and

(g) potential security risks.

21. Trusted Supplier Requirements

The Authority may establish a list or certification framework for suppliers authorised to provide critical IoT equipment to State institutions.

22. Prohibition of Defective or Non-Compliant Deployments

A person shall not knowingly supply or deploy critical IoT equipment that—

(a) contains known unmitigated critical vulnerabilities;

(b) lacks required security controls;

(c) cannot receive security updates where such updates are required;

(d) contains unauthorised malicious functionality; or

(e) materially fails applicable security standards.

23. Procurement Debarment

In addition to other penalties, a contractor found to have knowingly deployed materially defective or deliberately insecure infrastructure may be suspended or debarred from State procurement for a period prescribed by regulation or determined in accordance with applicable procurement law.

PART VI-
SECURITY TESTING AND INCIDENT RESPONSE

24. Security Assessment and Certification

The Authority may require specified classes of critical IoT infrastructure to undergo security assessment before deployment.

25. Independent Security Audits

High-risk critical infrastructure shall undergo periodic independent cybersecurity assessment as determined

26. Cybersecurity Incident Reporting

An operator shall notify the Authority of a material cybersecurity incident affecting critical IoT infrastructure within the period prescribed by regulation.

27. Critical Incident Notification

Where an incident presents an imminent threat to—

(a) life;

(b) public safety;

(c) electricity;

(d) water;

(e) transportation;

(f) healthcare;

(g) telecommunications; or

(h) other designated critical services,

the operator shall make an immediate preliminary notification to the Authority and provide further information as it becomes available.

28. Incident Response and Recovery

Operators shall maintain documented incident-response and disaster-recovery plans and shall conduct periodic testing.

29. Emergency Security Measures

Where there is an imminent and serious threat to critical infrastructure, the Authority may, subject to applicable law—

(a) direct an operator to isolate an affected device or network;

(b) require temporary suspension of a vulnerable system;

(c) require emergency firmware updates;

(d) require network segmentation;

(e) direct the preservation of relevant logs and evidence; or

(f) take any other proportionate measure necessary to protect critical infrastructure.

PART VII
REGULATORY SANDBOX

30. Edge Computing and IoT Regulatory Sandbox

The Authority may establish an Akwa Ibom Edge Computing and IoT Regulatory Sandbox to enable controlled testing of innovative technologies.

Participation may be made available to—

(a) start-ups;

(b) SMEs;

(c) universities;

(d) research institutions;

(e) technology companies; and

(f) public-sector innovators.

31. Research and Innovation Exemptions

The Authority may grant limited exemptions from specified requirements for controlled research or pilot projects where—

(a) the project does not create unacceptable risk;

(b) appropriate safeguards are implemented; and

(c) the exemption is time-limited.

PART VIII
PUBLIC AND CITIZEN PROTECTION

32. Protection of Citizens and Public Services

Operators shall take reasonable measures to prevent unauthorised manipulation of IoT systems that could—

(a) alter utility readings;

(b) disrupt public services;

(c) compromise public safety;

(d) expose personal information; or

(e) cause financial loss.

33. Protection Against Unauthorised Device Manipulation

A person shall not knowingly—

(a) gain unauthorised access to a critical IoT device;

(b) alter firmware without authorisation;

(c) disable security controls;

(d) manipulate telemetry;

(e) interfere with a critical edge node; or

(f) deploy malicious code against critical IoT infrastructure.

PART IX
ENFORCEMENT, OFFENCES AND PENALTIES

34. Compliance Notices

The Authority may issue a compliance notice requiring a person to remedy a contravention within a specified period.

35. Administrative Sanctions

The Authority may impose—

(a) warning;

(b) remediation order;

(c) mandatory security audit;

(d) suspension of deployment;

(e) withdrawal of certification;

(f) administrative monetary penalty;

(g) procurement suspension;

(h) procurement debarment; or

(i) referral to a competent law-enforcement authority.

36. Offences and Penalties

(1) A person who contravenes this Law for which no specific penalty is prescribed commits an offence and is liable on conviction—

(a) in the case of an individual, to a fine not exceeding ₦5,000,000 fine or confinement for a term not exceeding two years, or both; and

(b) in the case of a body corporate, to a fine not exceeding ₦20,000,000 fine.

(2) A person who knowingly deploys or supplies critical IoT infrastructure in material breach of mandatory security requirements is liable—

(a) individual: ₦5,000,000–₦20,000,000 fine or confinement up to three years, or both;

(b) body corporate: ₦20,000,000–₦50,000,000 fine.

(3) Where the breach causes substantial disruption, serious financial loss, physical harm, compromise of critical infrastructure or repeated violations—

(a) individual: ₦20,000,000–₦50,000,000 fine or confinement for three to seven years, or both;

(b) body corporate: ₦50,000,000–₦100,000,000 fine or an amount up to three times the financial benefit obtained or loss avoided, whichever is higher.

(4) A person who deliberately introduces malicious code, manipulates critical telemetry, compromises firmware or intentionally disrupts critical IoT infrastructure commits an offence and shall be liable to confinement for five to ten years, in addition to applicable fines.

(5) A continuing contravention may attract an administrative penalty of up to ₦500,000 fine per day after expiry of a valid compliance notice.

(6) The Court may order—

(a) restoration;

(b) remediation;

(c) compensation;

(d) replacement of defective infrastructure;

(e) forfeiture of proceeds;

(f) procurement debarment; or

(g) any other appropriate remedy.

37. Corporate Liability

Where an offence is committed by a body corporate, a director, manager, partner or senior officer who knowingly authorised, permitted or facilitated the offence may be personally liable.

38. Aggravating and Mitigating Factors

The Authority or Court shall consider—

(a) seriousness and duration;

(b) number of persons affected;

(c) criticality of the infrastructure;

(d) financial benefit obtained;

(e) actual harm;

(f) whether conduct was deliberate, reckless or negligent;

(g) previous violations;

(h) cooperation with authorities;

(i) voluntary disclosure; and

(j) remediation undertaken.

39. Restitution and Remediation

In addition to penalties, the offender may be required to bear reasonable costs of—

(a) incident response;

(b) forensic investigation;

(c) replacement of compromised devices;

(d) system restoration;

(e) security upgrades; and

(f) notification of affected persons.

40. Appeals

A person affected by an administrative decision under this Law may seek remedy in a competent court of Law.

PART X
FEES, FINANCE AND MISCELLANEOUS

41. Fees, Charges and Cost Recovery

(1) The Authority may prescribe reasonable fees for—

(a) registration;

(b) certification;

(c) security assessment;

(d) technical audits;

(e) regulatory sandbox participation;

(f) certification of testing laboratories;

(g) inspection; and

(h) other regulatory services.

(2) Recommended Initial Fees:

Service	**Suggested Maximum**
Non-commercial/research registration	**Nil**
Basic IoT registration	**₦100,000**
Critical IoT registration	**₦250,000**
High-criticality infrastructure registration	**₦500,000**

Service	Suggested Maximum
Security assessment	**₦250,000–₦1,000,000**
Certification	**₦100,000–₦500,000**
Renewal	**50% of applicable initial fee**
SME/start-up sandbox	**Nil**
Academic/public-interest sandbox	**Nil**
Large commercial sandbox	**Cost recovery**
Independent specialist assessment	**Actual reasonable cost**

42. Fund for Critical Digital Infrastructure Security

There shall be established, subject to applicable public-finance laws, a fund or budgetary mechanism for supporting—

(a) cybersecurity infrastructure;

(b) security testing laboratories;

(c) emergency incident response;

(d) capacity development;

(e) research and innovation;

(f) IoT security awareness;

(g) regulatory sandbox activities; and

(h) protection of critical State digital infrastructure.

43. Regulations

The Authority may make regulations concerning—

(a) IoT security standards;

(b) Edge Data Localization Zones;

(c) device certification;

(d) SBOM requirements;

(e) vulnerability disclosure;

(f) incident reporting;

(g) security audits;

(h) data classification;

(i) fees;

(j) procurement standards; and

(k) other matters necessary for implementation.

44. Confidentiality and Protection of Security Information

A person performing functions under this Law shall maintain confidentiality concerning sensitive security information obtained in the course of official duties, except where disclosure is authorised by law or necessary for the protection of critical infrastructure.

45. Cooperation with Federal Authorities

Nothing in this Law shall limit the powers of any competent Federal regulatory authority.

The Authority shall cooperate, where appropriate, with relevant Federal institutions responsible for—

(a) cybersecurity;

(b) telecommunications;

(c) data protection;

(d) critical infrastructure;

(e) electricity;

(f) financial services;

(g) national security; and

(h) law enforcement.

46. Limitation of Liability

No officer acting in good faith in the performance of functions under this Law shall be personally liable for an act or omission done in the lawful discharge of official functions, subject to applicable law.

47. Transitional Provisions

Existing critical IoT infrastructure deployed before commencement of this Law shall be brought into compliance within 12 months of commencement, or such longer period as the Authority may approve based on technical necessity and risk.Where immediate compliance is not technically practicable, the operator shall submit a remediation plan.

48. Savings

Nothing in this Law shall invalidate or affect any approval, licence, contract, intellectual property right, obligation, offence, penalty or liability created under the Act of the National Assembly.

49. Interpretation

In this Law—

"Authority" means the State Edge and IoT Security Authority established under this Law;

"Edge Computing" means the processing, analysis, storage or filtering of data at or near the location where the data is generated rather than exclusively within a centralised cloud or remote data centre;

"Edge Data Localization Zone" means a secure physical or logical environment designated by the Authority for the processing, storage or protection of specified critical State data;

"IoT device" means a physical device capable of collecting, processing, transmitting or receiving data through a network;

"Critical IoT Infrastructure" means an IoT system or network whose compromise, disruption or manipulation may materially affect public safety, essential services, public utilities, economic activity or government operations;

"smart meter" means an electronically connected device used to measure, record, transmit or manage the consumption or supply of electricity, water, gas or other public utilities;

"telemetry" means the automated collection and transmission of measurements, status information or operational data from remote devices;

"SBOM" means Software Bill of Materials;

"firmware" means software programmed into or embedded within a hardware device;

"OTA update" means an authorised over-the-air software or firmware update;

"critical data" means data designated as critical under this Law or regulations made under it.

50. Short Title

This Law may be cited as the Akwa Ibom State Edge Computing and Critical IoT Infrastructure Security Law, 2026.

SCHEDULE

SCHEDULE 1
CLASSIFICATION OF CRITICAL IoT INFRASTRUCTURE

Class I — Essential Critical Infrastructure, includes systems supporting:

(a) electricity generation, transmission and distribution;
(b) water supply;
(c) emergency services;
(d) healthcare;
(e) major transportation systems;
(f) critical government operations;
(g) public safety systems.

Class II — Critical Public Infrastructure, includes:

(a) smart-city systems;
(b) traffic management;
(c) public transportation;
(d) municipal utilities;
(e) environmental monitoring;
(f) public facilities;
(g) government telecommunications infrastructure.

Class III — Significant Infrastructure, includes other IoT systems whose compromise could cause material operational, economic or public-service disruption.

SCHEDULE 2
MINIMUM SECURITY CONTROLS

A Class I critical IoT deployment should, as applicable, include:

(a) unique device identity.
(b) strong authentication.
(c) encryption in transit.

(d) encryption at rest where appropriate.

(e) secure boot.

(f) signed firmware.

(g) secure OTA updates.

(h) vulnerability disclosure mechanism.

(i) Software bill of materials.

(j) network segmentation.

(k) access logging.

(l) tamper detection.

(m) backup and recovery.

(n) incident-response capability.

(o) defined security-support lifecycle.

(p) secure decommissioning.