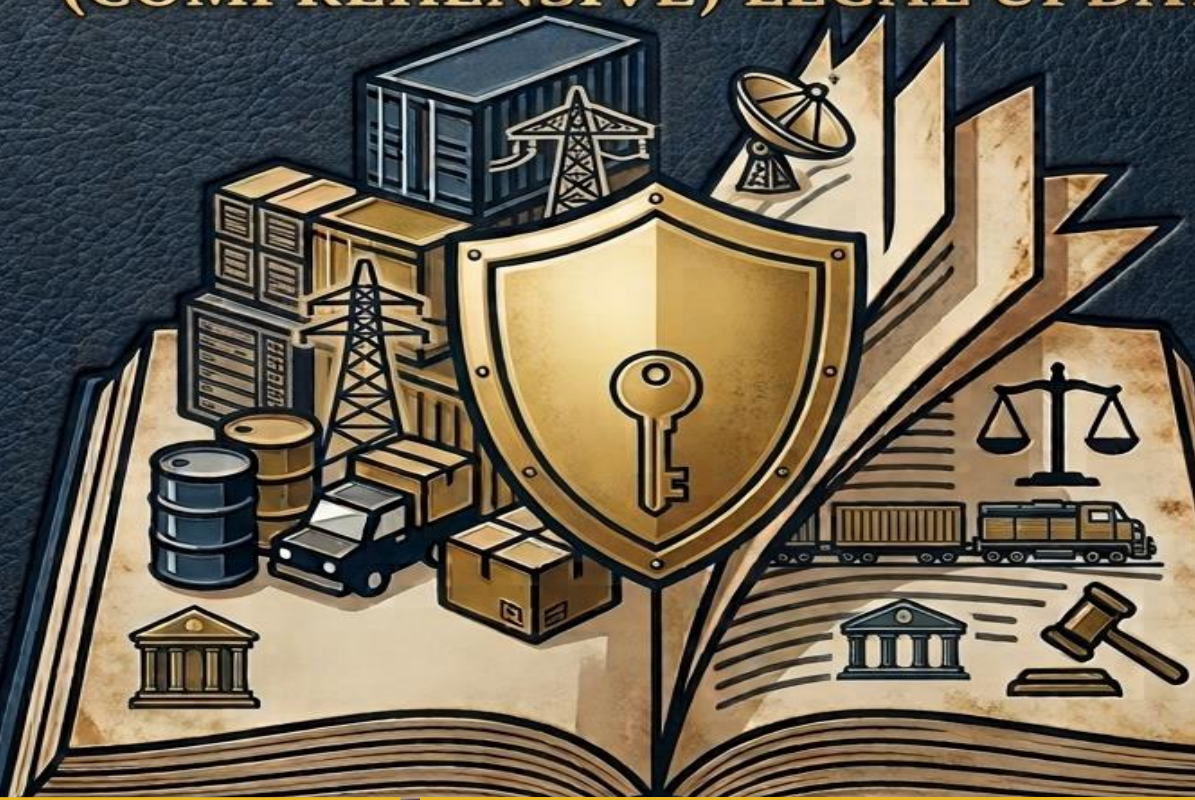
HIRKO & ASSOCIATES

ETHIOPIA'S CRITICAL INFRASTRUCTURE CYBERSECURITY PROCAMATION

PROCLAMATION NO. 1426/2026 (COMPREHENSIVE) LEGAL UPDATE



HIRKO & ASSOCIATES

LEGAL UPDATE: Ethiopia Enacts Critical Infrastructure Cybersecurity Proclamation

1. Introduction

The House of Peoples' Representatives has enacted the Critical Infrastructure Cybersecurity Proclamation No. 1426/2026, establishing a comprehensive legal framework for the protection of Ethiopia's strategic infrastructure from cyber threats. Published in the Federal Negarit Gazette on 21 July 2026, the Proclamation will enter into full force on 21 July 2027.

The legislation arrives amid Ethiopia's ongoing digital transformation, addressing the growing frequency and sophistication of cyberattacks targeting national infrastructure. During the first half of fiscal year 2025/2026 alone, the Information Network Security Administration recorded 27,773 cyberattacks. The Proclamation establishes obligations for infrastructure owners, creates a dedicated funding mechanism, introduces a licensing regime for cybersecurity service providers, and prescribes penalties for non-compliance.

2. Scope and Application

The Proclamation applies throughout Ethiopian territory and extends to designated critical infrastructures located outside the country. It also applies to persons providing cybersecurity products or services.

Critical infrastructure is defined as any public or private infrastructure or institution whose disruption or compromise due to a cyberattack would have a significant negative impact on national security or national interests. The definition encompasses both public and private entities operating in designated sectors.

The Proclamation identifies twelve critical infrastructure sectors: Information Technology and Communication, Finance, Security and Public Safety, Transport, Education, Health, Water and Energy, Government Services, Emergency and Disaster Response Services, Agriculture, Trade and Commerce, and Industry. The Administration retains authority to designate additional sectors through directives, subject to minimum criteria established in the Proclamation.

For infrastructure to be designated as critical, a cyberattack must pose a threat to the economy, social interaction, and daily life of the community, or adversely affect national security, peace and stability, diplomacy, or sovereignty. There must also exist a high level of interconnectedness such that damage would spread to other critical infrastructure sectors. Infrastructure that ceases to meet these requirements may be removed from critical infrastructure status following appropriate assessment by the Administration.

3. Obligations of Critical Infrastructure Owners

The Proclamation imposes eighteen core obligations on owners and operators of critical infrastructure, establishing a comprehensive framework for cybersecurity governance that requires substantial organizational commitment.

Infrastructure owners must formulate and implement cybersecurity programs based on national frameworks and develop their own frameworks based on policies and laws issued by the Administration. They are required to implement mandatory cybersecurity frameworks issued or recognized by the Administration. Owners must conduct regular cybersecurity risk assessments and impact analyses, participate in the National Cybersecurity Risk Survey conducted annually by the Administration, and provide relevant information.

Owners must obtain and renew cyber audit and cybersecurity inspection and evaluation certificates issued by the Administration. They must take appropriate corrective action based on audit findings within prescribed timelines. The use of information and communication technology systems that have not undergone cybersecurity inspection and evaluation is prohibited.

Infrastructure owners must employ cybersecurity professionals who have obtained professional certificates issued or recognized by the Administration. Existing professionals must obtain professional certification in accordance with established systems. Employees and officers with access to critical resources must obtain security clearance from the relevant government body.

Perhaps most significantly, infrastructure owners must notify the National Computer Emergency Response Center of cybersecurity incidents within 48 hours of detection and implement the solutions and directions provided. They must establish and manage centers responsible for monitoring, reporting, and responding to cyber attacks. Owners must ensure the security of technology product supply chains, and all new or upgraded information and communication technology systems acquired through purchase, donation, development, or any other means must obtain security clearance prior to implementation.

Infrastructure owners may implement these obligations by delegating to licensed cybersecurity service providers. However, the Administration shall identify critical infrastructure for which cybersecurity service shall not be provided by delegation on the grounds of national security and interests.

4. Role and Responsibilities of the Administration

The Information Network Security Administration exercises comprehensive authority under the Proclamation. The Administration formulates mandatory cybersecurity programs and monitors their implementation. It monitors and supports the development and implementation of cybersecurity programs by critical infrastructure organizations and oversees the implementation process of the National Cybersecurity Framework.

The Administration prepares an annual national cybersecurity risk, maturity, and security assessment report. It develops and implements cybersecurity drills and training in collaboration with various stakeholders, establishes and administers a National Cybersecurity Forum to enforce security and resilience in critical infrastructure, and provides access to cybersecurity frameworks, procedures, and important information using various methods.

Regarding cyber incident response, the Administration establishes systems for appropriate preemptive defense against attacks and coordinated incident response. It implements necessary monitoring and control measures to prevent cyber attacks, establishes information exchange platforms, and provides early warning of cyber incidents for critical infrastructure. The Administration coordinates national, regional, continental, and international cooperation on cyber incident prevention. It monitors and supervises procedures and implementations of organizations established to monitor, report, and respond to cyber incidents and issues directives to establish coordinated systems of procedures.

The Administration periodically discloses national cyber attack vulnerabilities, preventive measures, and timely security status reports to the public and conducts appropriate awareness raising activities.

The Administration conducts annual or ad hoc cybersecurity audits of critical infrastructure in accordance with national frameworks and international standards, issuing certification certificates to those who meet required standards. It authorizes private service providers to conduct cybersecurity audits and inspections.

5. Critical Infrastructure Cybersecurity Fund

The Proclamation establishes a permanent Critical Infrastructure Cybersecurity Fund to implement cybersecurity programs and frameworks designed to safeguard the security of key infrastructures. The Fund serves as a permanent source of financing for the implementation of its objectives.

The Fund supports the implementation of cybersecurity programs and frameworks developed by the Administration, research and development activities aimed at protecting critical infrastructure security, national and international training, drills, and capacity building programs to build the capacity of critical infrastructure institutions. It provides enabling infrastructures and platforms for activities carried out to protect the security of critical infrastructure, supports national campaigns and events organized to enhance cybersecurity awareness among citizens, and supports and coordinates initiatives and voluntary work undertaken by individuals, groups, or communities to ensure cybersecurity of critical infrastructure developments.

The Fund receives contributions from critical infrastructures as determined by Regulation issued by the Council of Ministers, voluntary support from institutions and individuals through fund raising programs, and revenues from service fees and administrative fines pursuant to the Proclamation. Funds obtained are deposited in a bank account opened by the Ministry of Finance. The Administration collects revenues at the end of each month and deposits them in the Fund account, notifying the Ministry of Finance within seven days of receiving revenue. The administration, utilization, and detailed operational procedures of the Fund shall be determined by Regulation to be issued by the Council of Ministers.

6. Licensing of Cybersecurity Service Providers

The Proclamation introduces a comprehensive licensing regime for cybersecurity service providers. Any person seeking to provide cybersecurity products or services must obtain a license from the Administration. Provision of cybersecurity products or services without a valid license is prohibited.

Applicants must possess legal entity status, obtain appropriate security clearance, meet requirements for professionals, technology, and operational systems necessary to provide the service, possess minimum capital and provide commensurate guarantee, maintain a permanent address in Ethiopia, not have lost all or part of capacity in judgment or law, and have never been convicted of crimes related to fraud, corruption, or breach of trust. Detailed requirements shall be determined by directive issued by the Administration.

Licensed persons must use the license only for the purpose and scope for which it is authorized and may not transfer, lend, or allow a third party to use the license without notifying or obtaining permission from the Administration. They must notify the Administration immediately when there is a change in licensing requirements, keep confidential information obtained in the course of their duties, provide necessary information requested by the Administration in the discharge of its supervisory responsibilities, and comply with the Proclamation and other obligations set out in Regulations and Directives.

The Administration may suspend a license for up to sixty consecutive days where there is reasonable ground to believe that grounds for revocation exist, pending investigation and verification. If the Administration

confirms suspected offenses have been committed, it shall revoke the license. If the offense is found to be minor, the matter may be dismissed with a warning. Licenses may be revoked where information provided is fraudulent, the license is used outside its authorized scope, the licensed person violates implementing instruments, the license expires without renewal, the licensed person dies or loses capacity or the organization dissolves or is declared bankrupt, the licensed person is convicted of fraud or breach of trust, licensing requirements are not met, or the licensee ceases to provide service.

The Administration shall establish a system for the issuance of professional certifications or accreditations to cybersecurity professionals performing cybersecurity functions within critical infrastructure.

7. Penalties and Enforcement

The Proclamation establishes administrative penalties for violations of its provisions. Infrastructure owners who fail to implement mandatory cybersecurity frameworks in a timely manner face fines of 500,000 to 1,000,000 Birr. Failure to notify cybersecurity incidents to the National Computer Emergency Response Center within 48 hours or failure to take appropriate corrective action attracts fines of 1,500,000 to 2,000,000 Birr. Failure to provide necessary information or cooperate with the National Computer Emergency Response Center results in fines of 300,000 to 500,000 Birr.

8. Conclusion

The Critical Infrastructure Cybersecurity Proclamation No. 1426/2026 establishes a comprehensive legal framework for the protection of Ethiopia's critical infrastructure from cyber threats. The legislation imposes substantial obligations on infrastructure owners, creates a dedicated funding mechanism, introduces a licensing regime for service providers, and prescribes significant penalties for non-compliance. The one-year transition period provides institutions with an opportunity to prepare for full compliance. Organizations operating in designated critical infrastructure sectors should assess their current cybersecurity posture against the Proclamation's requirements and develop implementation strategies.

Disclaimer

This legal update is provided for informational purposes only and does not constitute legal advice. Organizations should consult with qualified legal and cybersecurity professionals for guidance specific to their circumstances.

Hirko & Associates Law Office

Addis Ababa, Ethiopia