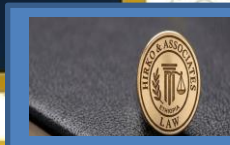


Hirko and Associates (HALO) Legal Update

WHAT EVERY IMPORTER, IT BUSINESS, AND ORGANIZATION SHOULD
KNOW ABOUT ETHIOPIA'S IT PRODUCT SECURITY LAW



INFORMATION TECHNOLOGY PRODUCTS SECURITY CLEARANCE AND CONTROL PROCLAMATION NO. 1310/2023: WHAT STAKEHOLDERS SHOULD KNOW

1. Introduction

Ethiopia's digital transformation has accelerated the adoption of information technology across government institutions, businesses, financial services, and everyday commercial activities. As technology increasingly underpins critical infrastructure and economic development, the need for a legal framework capable of safeguarding national information security has become equally important.

Against this background, Ethiopia enacted the **Information Technology Products Security Clearance and Control Proclamation No. 1310/2023**, which entered into force on 6 March 2024. While the Proclamation has been in effect for some time, it continues to carry significant practical implications for importers, technology companies, manufacturers, software developers, businesses, and users of information technology products. Nevertheless, many organizations remain unfamiliar with the breadth of its application and the compliance obligations it imposes.

This article revisits the key features of the Proclamation and highlights the principal issues that stakeholders should understand when engaging in activities involving information technology products in Ethiopia.

2. Purpose of the Proclamation

The Proclamation establishes a legal framework for regulating information technology products that may pose risks to Ethiopia's information security. It seeks to protect national information infrastructure from technological threats by introducing a system for identifying products that present security concerns and regulating their manufacture, importation, exportation, distribution, possession, and use.

To achieve these objectives, the law empowers the Information Network Security Administration (INSA) to identify prohibited and restricted products, issue security clearance permits, supervise regulated activities, and enforce compliance through inspections and other regulatory measures.

3. A Broad Scope of Application

One of the defining characteristics of the Proclamation is its broad scope. Rather than focusing solely on computer hardware or networking equipment, the legislation adopts an expansive definition of "Information Technology Product." It encompasses technologies capable of infiltrating, intercepting, disrupting, manipulating, destroying, or otherwise compromising electronic data and information systems.

Similarly, the Proclamation extends beyond importation activities. It regulates a wide range of activities involving covered products, including manufacturing, assembly, sale, exchange, possession, promotion, utilization, and exportation. Consequently, businesses operating at different stages of the technology supply chain should carefully assess whether their products or activities fall within the scope of the legislation.

4. Prohibited Vs Restricted Products

The regulatory framework established by the Proclamation distinguishes between prohibited products and restricted products.

Prohibited products are technologies that may not be imported, manufactured, sold, possessed, exported, or used because of the level of information security risk they present. Restricted products, on the other hand, are not entirely prohibited but may only be imported, exported, manufactured, sold, or utilized after obtaining the appropriate security clearance permit from INSA.

The identification of these products is not static. The Proclamation authorizes INSA, in collaboration with relevant government institutions, to periodically identify, revise, and publish the list of prohibited and restricted products through directives. Accordingly, compliance requires continuous monitoring of subsequent regulatory instruments in addition to the Proclamation itself.

5. The Security Clearance Regime

A central feature of the Proclamation is the establishment of a security clearance system for restricted products. Depending on the nature of the regulated activity, permits may be required before products are imported, exported, manufactured, sold, or otherwise used.

Obtaining a permit is not the end of the regulatory process. Permit holders are required to comply with continuing obligations regarding the lawful use, security, record keeping, and management of the permitted products. The law further authorizes INSA to suspend or revoke permits where statutory requirements are no longer satisfied or where permit conditions are violated.

6. Regulatory Oversight and Enforcement

The Proclamation provides INSA with extensive supervisory and enforcement powers intended to ensure effective implementation of the law. These powers include conducting inspections, monitoring compliance, investigating suspected violations, and coordinating with customs authorities and other government institutions in controlling regulated products.

Where the legal requirements are not observed, the law authorizes administrative and criminal enforcement measures. Depending on the nature of the violation, consequences may include confiscation of products, suspension or revocation of permits, administrative fines, and criminal penalties, including imprisonment for serious offences involving prohibited or unauthorized restricted products.

7. Practical Implications for Stakeholders

The Proclamation has practical implications for a broad range of stakeholders operating within Ethiopia's technology ecosystem. Importers and distributors should ensure that products intended for importation have been assessed against INSA's regulatory requirements before shipment. Technology companies and software developers should evaluate whether the technologies they develop, supply, or integrate fall within the scope of the regulatory framework. Organizations procuring information technology products should also incorporate regulatory due diligence into their procurement and compliance processes to ensure that the products they acquire can be lawfully imported and used within Ethiopia.

Given that INSA is empowered to issue implementing directives and periodically revise the list of regulated products, compliance should be viewed as an ongoing obligation rather than a one-time exercise.

8. Conclusion

The Information Technology Products Security Clearance and Control Proclamation No. 1310/2023 represents a significant development in Ethiopia's information security and technology regulatory landscape. Although the Proclamation is no longer a recent legislative development, its practical importance remains substantial as organizations continue to expand their reliance on digital technologies.

For businesses operating in Ethiopia, compliance with the Proclamation requires more than a general awareness of its existence. It calls for a careful assessment of technology-related operations, procurement practices, and regulatory obligations to ensure that activities involving information technology products are conducted within the framework established by the law. As Ethiopia's digital economy continues to evolve, understanding and complying with this regulatory regime will remain an important component of sound legal and corporate governance.

Disclaimer:

This publication is intended solely for general informational purposes and should not be construed as legal advice. Specific legal advice should be obtained based on the particular facts and circumstances of each case.