



AMAN &
PARTNERS

LEGAL
UPDATE
ISSUE 12

REFLECTIONS ON THE
INFORMATION TECHNOLOGY
PRODUCTS SECURITY CLEARANCE
AND CONTROL PROCLAMATION

MARCH 2024

Information Technology (IT) is transforming rapidly in ways that enhance the efficiency of many economic sectors, including agriculture, education, healthcare, finance, marketing, and beyond. On the other hand, IT products are prone to misuse and pose vulnerability against nations, the business community, and individuals. This vulnerability can result in various damages, such as data breaches, system disruptions, and economic losses. As a result, with a view to ensuring IT products are deployed for their utmost use and to mitigating risks, countries have used various strategies, including the enactment of laws regulating the import, export, invention, and use of these products.

The Ethiopian parliament recently approved the Information Technology Products Security Clearance and Control Proclamation No. 1310/2023 (ITPS Proclamation). According to the ITPS Proclamation, the rationale behind adopting this law is to lay down a clear system to identify, inspect and follow up the import, export and use of regulated IT products and put in place a system for issuing certification of security clearance so that the country's information resources and security of citizens would be protected, and attacks minimised.

This legal update explores the ITPS Proclamation governing the importation, exportation, production, possession, and use of IT products in Ethiopia.

Regulated IT Products and Activities and Regulatory Powers

According to the ITPS Proclamation, IT products that are regulated include “any technology device, design, algorithm, method, service, or application that can infiltrate, disrupt, intercept, destroy, mislead, distort, steal, and falsify electronic data or signals.” In addition, activities related to the import, export, manufacturing, innovation, sale, exchange, possession, promotion, use and facilitating the use of these IT products for any purposes except for the purpose of education, or research and development are regulated. The scope of the ITPS Proclamation is limited to IT products that can potentially pose security threat. IT products that don't pose threat to the information resource of the nation and its citizen will not be subject to regulation. That said, the ITPS Proclamation does not provide a list of IT products that pose security threats.

The ITPS Proclamation mandates the Information Network Security Administration (INSA) to identify and list IT products that are subject to prohibition and regulation through a directive. In so doing, INSA is required to collaborate with National Intelligence Security Service (NISS) and other concerned bodies. The ITPS Proclamation requires that such list be subject to annual regular revision in ways that take the dynamism and advancement of the technologies into account.

Even before the enactment of the ITPS Proclamation, INSA, in collaboration with other authorities, has been controlling, registering and licensing import, export and use of variety of IT products, information sensor, surveillance cameras, walkie-talkie radio, telecom products, antenna, VSAT, BGAN, satellite phones, compass and GPS products, high-capacity mining servers, cryptographic products, drones and others that are allegedly potential threats to the country's security and economy. INSA has been conducting this task based on the mandate given to it under the Information Network Security Agency Re-establishment Proclamation No. 808/2013 (INSA Establishment Proclamation). This law in general mandated INSA to control import, export, and use of IT products.

However, INSA Establishment Proclamation does not provide details based on which INSA would operate in regulating these activities. In addition, the INSA Establishment Proclamation does not provide guidance on the type of IT products that would be prohibited or permitted for use and the consequences for breach of these laws. Therefore, the purpose of the enactment of the ITPS Proclamation is largely to provide details on regulatory powers of INSA, guidance on the type of IT products to be permitted or prohibited and set out corrective actions and consequences for breach of the law.

Security Clearance Permits

According to the ITPS Proclamation, IT products and related activities are required to obtain security clearance permit from INSA. The types of permits include pre-import, import, export, manufacturing, sale and permits for use of other regulated activities.

The permit holder is obliged to use the permit only for the intended purpose and for the authorised scope. The permit holder should refrain from transferring products to any third party without prior authorisation from INSA. Furthermore, in the event of loss, theft, damage, or loss of control over the product, the permit holder is responsible for promptly notifying INSA within 8 hours from becoming aware of the occurrence of the event.

INSA is required to designate inspectors and setup a standardised control mechanism at the entry and exit customs checkpoints of the country. Where it has suspected that there is unauthorised possession and use of the IT products, it can search a premise with a court order. In case of imminent information security risk, it is authorised to conduct the search without a court order and notify the same within 48 hours to a nearby court.

It is important to note that obtaining security clearance permit from INSA does not necessarily allow the deployment of the IT product. The clearance requirement under the ITPS Proclamation is in addition to the requirement for obtaining approval, if any, from other regulatory bodies, including the Ethiopian Communication Authority and the Ethiopian Media Authority.

Consequences of Non-compliance

Violation of the ITPS Proclamation and its implementation Regulations and Directives entails administrative and criminal penalties. The ITPS Proclamation empowers INSA together with the Customs Commission to forfeit illegally used IT products. Measures to suspend and revoke the security clearance permit could also be taken. Furthermore, non-compliance could result in imprisonment ranging from simple imprisonment to rigorous imprisonment; and a fine. The penalties vary depending on factors such as the type of the activities, the level of negligence, the absence of harm caused to citizens and the country, and the number of IT products deployed or the nature of the offence.

Concluding Remarks

The enactment of the ITPS Proclamation is a step towards setting clear standards to regulate the deployment, innovation, importation and exportation of IT products in the context of Ethiopia. That said, the issuance of INSA's directive contemplated under the ITPS Proclamation is critical in operationalising the rules laid down under the Proclamation. While the implications of the ITPS Proclamation would be clearer once its subsidiary legislation is issued and implemented, various actors in this area should be aware that the implementation of the law is likely to affect the business-as-usual operations, resulting in cost escalation throughout the supply chain and possible disruptions in their business operations if security clearance permit is not obtained. As such, businesses, particularly IT product importers, manufacturers, service providers and users need to closely follow developments in the issuance and implementation of future subsidiary legislations of the ITPS Proclamation. Businesses should also pay particular attention to whether other approvals from other government authorities, including the Ethiopian Communications Authority, are required before the deployment of IT products.



AMAN & PARTNERS LEGAL SERVICE LLP

info@aaclo.com | www.aaclo.com

DISCLAIMER

The information contained in this legal update is only for general information purposes. Nothing herein shall be considered and relied upon as a legal advice or a substitute thereto.

© Aman & Partners LLP. All Rights Reserved 2023

