Energy Practice
Issue 3 | February 2022

DESIGNATION OF CRITICAL INFRASTRUCTURE IN KENYA

Introduction

On January 31st, 2022, the National Computer and Cybercrimes Co-ordination Committee designated various categories of infrastructure as critical infrastructure with effect from January 20th, 2022. This was effected vide Gazette Notice No. 1043 published under the Computer Misuse and Cybercrimes Act, No. 5 of 2018 which was enacted in 2018 to provide for offences relating to computer systems, to enable timely and effective detection, prohibition, prevention, response, investigation and prosecution of computer and cybercrimes and to facilitate international co-operation in dealing with computer and cybercrime matters.

The designation of critical infrastructure comes in the wake of several instances of vandalism to specific infrastructure in the energy sector that saw the vast population plunged into darkness for several hours at a time in the course of December 2021 and January 2022, which incidents have been attributed to the scrap metal industry. In her 1st Energy Briefing of 2022, the Cabinet Secretary for Energy sought to reassure key stakeholders that the sector infrastructure, particularly the transmission network, was indeed secure and emphasis would be placed on ensuring that these incidents did not occur future.

Telecommunications, Electricity and Water Infrastructure among those designated as critical infrastructure under the Computer Misuse and Cybercrimes Act

Designated Infrastructure

Section 9 of the Act obliges the Director of the National Computer and Cybercrimes Co-ordination Committee to designate certain systems as critical infrastructure, that is, those processes, systems, facilities, technologies, networks, assets and services essential to the health, safety, security or economic well-being of Kenyans and the effective functioning of Government. In determining if a system is critical, regard has to be had to whether a disruption in the system would result in: (a) the interruption of a life sustaining service including the supply of water, health services and energy; (b) an adverse effect on the economy of the Republic; (c) an event that would result in massive casualties or fatalities; (d) failure or substantial disruption of the money market of the Republic; and (e) adverse and severe effect of the security of the Republic including intelligence and military services.

Key Sector Categories

Critical services have been categorized into five key sectors including the telecommunications sector which incorporates voice/data communication, internet connectivity, domain and IP management as well as data and information management. Key infrastructure includes mobile communication infrastructure/systems, International Internet Gateways, Internet Exchange Points and Mobile Internet Networks, systems supporting DNS and IP functions as well as data centres, in-country cloud infrastructure amongst others.

In the Electoral, Judicial, Education, Health, Food, Water and Land sector, of interest in the water sub-sector is systems supporting water storage, water distribution, water quality assurance, wastewater collection and treatment which have been designated as critical. The Energy, Transport and Industry Sector includes road transport services, cargo management, air navigation, airports operation, power generation, power transmission and distribution, petroleum transportation, storage and distribution as well as manufacturing, processing and assembling services. Of particular interest to

participants in the energy sector would be the Energy Generation Systems including full reduction of Geothermal Fluid System, working fluid system, cooling system, hydropower ICT systems; systems supporting and managing power transmission/distribution and billing; and systems that support/enable safe and effective transportation, storage and distribution and use of large volumes of petroleum products.

The other designated sectors include banking and finance sector and the defence, security and public safety sector. Within the public and environmental safety subsector, sector players should note that designated systems include those supporting public safety and emergency response, surveillance, incident response, air pollution monitoring, early warning, meteorological monitoring and ground water (lake/river) monitoring amongst others.

Key Obligations of Infrastructure Owners

Following designation of critical infrastructure, the Director is obliged under Section 9(4) of the Act to issue various directives regulating, *inter alia*, the classification of data held by the critical information infrastructure, the protection of, the storing of and archiving of data held by the critical information infrastructure, cyber security incident management by the critical information infrastructure; disaster contingency and recovery measures, which must be put in place by the critical information infrastructure and minimum physical and technical security measures that must be implemented in order to protect the critical information infrastructure. The directives should also indicate the period within which the owner, or person in control of a critical information infrastructure must comply with the directives.

Owners of critical infrastructure obliged to conduct risk assessments and submit annual compliance reports

Section 10 of the Act provides that the Committee shall, in consultation with a person that owns or operates the critical information infrastructure, conduct an assessment of the threats, vulnerabilities, risks, and probability of a cyberattack across all critical infrastructure sectors as well as determine the harm to the economy that would result from damage or unauthorized access to critical infrastructure. The Committee is also obliged to recommend to the owners of systems designated as critical infrastructure, methods of securing their systems against cyber threats.

The owner or operator of a system designated as critical infrastructure is required under Section 11 of the Act to report to the Committee any incidents likely to constitute a threat in the nature of an attack that amounts to a computer and cybercrime and the action the owner or operator intends to take to prevent the threat and the National Security Council is obliged to provide technical assistance to the owner or operator of a critical infrastructure to mitigate the threat reported to Committee.

Finally, the owners of critical infrastructure are obliged to submit a compliance report on the critical information infrastructure to the Committee annually in line with a critical infrastructure framework in order to evaluate compliance.

Concluding Remarks

The designation of critical infrastructure is a welcome development in light of the increasing need to better protect these systems from disruption by natural disasters and man-made threats including terrorism, cyber-attacks, disinformation, hostile foreign ownership and physical vandalism of critical assets. It is important that the directives that will now be issued under Section 9 of the Act recognise the increasing interdependencies and evolving risks arising due to the various categories of infrastructure being more reliant upon one another and that disruptions in one sector can have immediate, and in some cases, long-lasting effects on operations in others. Moreover, some of the disruptions can also have severe and cross-border consequences for security, and lead to uncertainty or undermine confidence in the

responsible authorities and providers of essential services. It is therefore hoped that the ensuing directives will provide the mechanism necessary for owners to identify and manage these interdependencies in a systematic way.

It is noted that the Act places a strong emphasis on risk identification and protection of the critical infrastructure against threats and attacks but does not address issues relating to the resilience of such infrastructure, that is, the capability to quickly bounce back in the wake of disruptions – whether due to natural disasters or man-made threats and actions. It is therefore hoped that the directives will indeed address both the protection of the critical assets as well as their resilience in the long term.

Finally, it is noted that the designation was published on January 31st, 2022, but the effective date was recorded as January 22nd, 2022. While the Statutory Instruments Act. No. 13 of 2013 provides that a statutory instrument shall come into operation on the date specified and that it may be made to operate retrospectively, it is important to note that no person can be liable to a penalty in respect of any contravention of a provision in a statutory instrument required to be published in the Gazette where the alleged contravention occurred before the publication unless the court is satisfied that before the alleged contravention, the purport of the statutory instrument had been brought to that person's notice.

Mary Chege
mary.chege@emsi.co.ke

Maryanne Wachira
brenda.cheptoo@emsi.co.ke