Annex 1

ITU Regional Development Forum for Arab Region (RDF-ARB)

Accelerating the digital development in Arab Region

Organized by the International Telecommunication Union with the support of the

Bahraini Ministry of Transportation and Telecommunications

6-8 November 2023 - Kingdom of Bahrain

CONTRIBUTION FORM

Please note that submitted information will be presented during the RDF-ARB P2C Roundtables and it will also be reflected on the pledging platform of the Partner 2 Connect Digital Coalition.

Once completed send to ITU-RO-ArabStates@itu.int

ORGANIZATION: National Communications Authority (NCA) of Somalia

FOCAL POINT: Ms Naima Hassan Dimbil, Director of Interconnection, wholesale and Universal access Department National Communications Authority (NCA) of Somalia

TITLE: Somalia national cybersecurity strategy development

DESCRIPTION OF ACTION:

-- Developing a National Cybersecurity Strategy for Somalia is a critical initiative aimed at protecting the country's digital infrastructure, data, and national security interests. Somalia's strategy development will be via the following pillars :

1. Stakeholder Engagement:

The development of a National Cybersecurity Strategy begins with extensive stakeholder engagement. This includes government agencies, law enforcement, private sector organizations, academia, civil society, and international partners. These stakeholders collaborate to identify the country's specific cybersecurity challenges, needs, and priorities.

2. Risk Assessment:

A comprehensive risk assessment is conducted to identify potential threats, vulnerabilities, and risks to Somalia's critical information infrastructure. This involves evaluating the current state of

cybersecurity, potential attack vectors, and the potential impact of cyber threats on national security, the economy, and public safety.

3. Define Goals and Objectives:

Based on the risk assessment, clear and measurable goals and objectives are established. These goals often include enhancing cybersecurity resilience, protecting critical infrastructure, and fostering collaboration among stakeholders.

4. Legal and Regulatory Framework:

An effective National Cybersecurity Strategy often includes the development or enhancement of legal and regulatory frameworks. This might include passing cybersecurity laws and regulations that define the roles and responsibilities of various stakeholders, as well as provisions for incident reporting and response.

5. Capacity Building:

To implement the strategy, a focus on capacity building is crucial. This includes training and developing a cybersecurity workforce, raising awareness about cybersecurity best practices, and providing technical assistance to relevant organizations.

6. Incident Response Plan:

A critical component of the strategy is the development of an incident response plan. This outlines the procedures for detecting, reporting, and responding to cyber incidents. It includes the establishment of a Computer Incident Response Team (CIRT) to coordinate responses and mitigate threats effectively.

7. Public Awareness and Education:

Efforts to raise public awareness and educate citizens about cybersecurity are essential. This may involve public awareness campaigns, cybersecurity training, and educational programs targeting schools, businesses, and individuals.

8. Collaboration and Information Sharing:

The strategy promotes collaboration with international partners and organizations. This involves sharing threat intelligence, best practices, and cooperating on cybersecurity initiatives to address cross-border threats effectively.

9. Monitoring and Evaluation:

Regular monitoring and evaluation of the strategy's implementation are crucial to ensure its effectiveness. Key performance indicators (KPIs) are established to measure progress, and adjustments are made as necessary to respond to emerging threats and challenges.

10. International Cooperation:

Cyber threats often transcend national borders, making international cooperation essential. Somalia's strategy should include provisions for working with regional and international organizations and partners to combat cybercrime and enhance cybersecurity.

The development of a National Cybersecurity Strategy for Somalia is a dynamic and ongoing process that requires continuous adaptation to the evolving cyber threat landscape. It should be a living document that is regularly updated to address emerging challenges and leverage new technologies and best practices to protect the country's digital infrastructure and national security interests.

COUNTRIES in FOCUS: [Name countries to be impacted by this action]

Somalia

YEARS of IMPLEMENTATION: [Tick the relevant boxes or delete the irrelevant items]

☐ 2023

☒ 2024

☒ 2025

RELEVANT ITU REGIONAL INITIATIVE: [Tick the relevant boxes or delete the irrelevant items]

☐ ARB1: Sustainable digital economy through digital transformation.

including Pacific Island countries, and landlocked developing countries

☒ ARB2: Enhancing confidence, security and privacy in the use of telecommunications/Information and communication technologies in the era of new and emerging digital technologies.

☐ ARB3: Developing digital infrastructure for smart sustainable cities and communities.

☐ ARB4: Building capacities and encouraging digital innovation, entrepreneurship and future foresight.

☐ ARB5: Developing means of digital regulation.

Please find more information on the ITU Regional Initiatives 2023-2025, as defined by WTDC-22,

https://www.itu.int/en/ITU-D/Pages/regional-initiatives-2023-2025.aspx

RELATED ITU-D PRIORITIES AS DEFINED BY THE ITU WORLD TELECOMMUNICATION DEVELOPMENT CONFERENCE 2022

☐ Affordable connectivity

☐ Digital Transformation

☐ Enabling policy and regulatory environment

☐ Resource mobilization and international cooperation

☒ Inclusive and secure telecommunications/ICTs for sustainable development

Please find more information on the ITU-D Priorities, as defined by WTDC-22, here

RELATED ITU PRIORITIES AS DEFINED BY ITU PLENIPOTENTIARY CONFERENCE 2022

☐ Spectrum use for space and terrestrial services.

☐ International telecommunication numbering resources.

☒ Inclusive and secure telecommunication/ICT infrastructure and services.

☐ Digital applications.

☐ Enabling environment.

Please find more information on the ITU Priorities, as defined by PP-22, here