



Federal Republic of Somalia
Ministry of Communications and Technology (MoCT)

Terms of Reference (ToR)

For the Position of

Cybersecurity Capacity Development Specialist

in Support of The National Communications Authority (NCA), FGS

Eastern Africa Regional Digital Integration Project (EARDIP)

Project ID: P176181

1. BACKGROUND

The Federal Government of Somalia has received a grant from the International Development Association (IDA) of the World Bank toward the cost of the Eastern Africa Regional Digital Integration Project (EA-RDIP), with the Ministry of Communications and Technology (MoCT) serving as the implementing agency. EA-RDIP addresses the connectivity needs of the Horn of Africa region and aims to advance the integration of digital markets in Eastern Africa—supporting cross-border connectivity, harmonizing data and e-commerce regulations, and removing trade barriers toward the vision of a Single Digital Market (SDM). Delivered through a regional Series of Projects (SOP) approach involving both countries and regional economic communities, the first phase (SOP-I) covers the East African Community (EAC) and the Intergovernmental Authority on Development (IGAD), together with Somalia and South Sudan, enabling these countries to catch up with their regional peers. Under SOP-I, EA-RDIP supports the Federal Government of Somalia through a USD 80 million operation, structured around four components: (1) Connectivity Market Development and Integration; (2) Data Market Development and Integration, including cybersecurity; (3) Online Market Development and Integration; and (4) Project Management and Implementation.

As a key institution in delivering EA-RDIP, the National Communications Authority (NCA)—the independent regulator of Somalia's communications sector, established under the National Communications Act of 2017—licenses operators and regulates telecommunications, Internet, broadcasting, ICT and eCommerce services; manages radio-frequency spectrum and the national numbering plan; promotes fair competition; and protects consumer rights. To support the

implementation of the project and the regulatory reforms underpinning Somalia's integration into the regional digital market, the NCA requires a dedicated Cybersecurity Capacity Development Specialist to serve as a Cybersecurity Capacity Development Specialist to support the implementation of national cybersecurity initiatives, institutional capacity development, workforce enhancement, cybersecurity awareness programs, and cyber resilience initiatives in Somalia. The Specialist will serve as the National Communications Authority's focal point for engagement with global digital and social media platforms, supporting the establishment and maintenance of effective relationships with major online service providers operating in Somalia. The Specialist aims to strengthen cybersecurity awareness, workforce development, institutional readiness, cyber resilience, and technical capabilities across government institutions, private sector entities, academia, and other critical stakeholders.

The specialist will support the implementation of national cybersecurity priorities and initiatives under the leadership of the NCA and contribute to strengthening Somalia's cybersecurity ecosystem, operational readiness, and national cyber resilience capabilities.

2. SPECIFIC TASKS UNDER THIS PHASE OF THE PROJECT INCLUDE:

- Develop a National Cybersecurity Capacity Development Framework and implementation roadmap.
- Support SOMCIRT operational readiness and cybersecurity workforce development initiatives.
- Facilitate cybersecurity training and technical workshops for public and private sector institutions.
- Conduct CyberDrills, tabletop exercises, and incident response simulation exercises.
- Support cybersecurity workforce development and professional certification initiatives.
- Conduct institutional cybersecurity readiness and skills gap assessments.
- Coordinate and organize the annual Somali National Cybersecurity Forum and cybersecurity awareness events.
- Facilitate partnerships and cooperation with regional and international cybersecurity organizations, CERTs, and CIRTs.
- Promote cybersecurity information sharing, collaboration, and stakeholder coordination mechanisms.
- Support cybersecurity resilience and incident response coordination initiatives under SOMCIRT.
- Provide technical advisory support to government institutions and stakeholders on cybersecurity matters.
- Organize cybersecurity innovation and youth engagement initiatives to strengthen national cybersecurity talent development.

Please note that it is expected that the task will be carried out primarily in English and Somali.

3. DELIVERABLES

The primary deliverables (to be updated at different stages during the process) are:

- Develop a National Cybersecurity Capacity Development Framework and implementation roadmap.
- Support the operational readiness, institutional strengthening, and human capacity development of SOMCIRT.
- Design and implement nationwide cybersecurity awareness campaigns targeting government institutions, academia, private sector entities, and the public.
- Conduct cybersecurity training programs for NCA departments, technical staff, government institutions, private sector entities, and relevant stakeholders.
- Conduct cybersecurity workshops, awareness sessions, tabletop exercises, CyberDrills, simulation exercises, and technical training programs.
- Develop cybersecurity training manuals, educational materials, operational guidelines, awareness content, and technical documentation.
- Conduct institutional cybersecurity capacity and readiness assessments.
- Support SOMCIRT incident response preparedness and cybersecurity operational capability development.
- Develop recommendations for cybersecurity workforce development and professional certification pathways.
- Coordinate and facilitate the annual Somali National Cybersecurity Forum, CyberDrills, and stakeholder engagement activities.
- Facilitate cooperation and partnership initiatives with regional and international cybersecurity organizations and CERTs/CIRTs.
- Support the establishment of cybersecurity information-sharing and coordination mechanisms among stakeholders.
- Provide technical support and advisory services to relevant government institutions and stakeholders on cybersecurity best practices and cyber resilience initiatives.
- Organize cybersecurity awareness campaigns, public outreach programs, and cybersecurity innovation initiatives.
- Prepare periodic progress reports and technical documentation related to cybersecurity capacity-building activities.
- Submit a Final Assignment Report including key achievements, lessons learned, recommendations, and future strategic priorities.

4. REQUIRED QUALIFICATIONS AND EXPERIENCE

The individual consultant should be able to offer all, or at least most, of the following qualifications and experience:

- Candidate must possess a postgraduate degree in Cybersecurity, Information Security, Computer Science, Information Technology, Telecommunications, Digital Transformation, or related field, with a minimum of 5 years of relevant professional experience in cybersecurity capacity development, cybersecurity awareness, SOMCIRT/CERT operations, or ICT security leadership roles in either the public or private sectors.

- Relevant experience in cybersecurity capacity-building initiatives, ICT development programs, digital transformation projects, telecommunications, regulatory institutions, academia, international organizations, or consultancy assignments.
- Demonstrated experience in designing and implementing cybersecurity awareness campaigns, workforce development programs, institutional strengthening initiatives, and cybersecurity training activities.
- Proven experience in organizing cybersecurity trainings, workshops, CyberDrills, conferences, stakeholder engagement programs, and cybersecurity awareness events.
- Experience supporting National CERT/CIRT establishment, operational readiness, cyber incident response coordination, or cybersecurity institutional development initiatives will be an added advantage.
- Strong understanding of international cybersecurity standards, frameworks, and best practices, including ISO/IEC 27001, NIST Cybersecurity Framework, ITU cybersecurity capacity-building initiatives, and related frameworks.
- Experience in cyber incident response coordination, cyber resilience programs, threat information sharing, and cybersecurity operational readiness initiatives is highly desirable.
- Demonstrated capability to coordinate with government institutions, academia, development partners, regional organizations, private sector stakeholders, and international cybersecurity communities.
- The Candidate should have work experience and in-depth knowledge of Somalia generally and a sensitivity to the underlying state of fragility and prevailing challenges in particular.
- Demonstrated ability to communicate effectively in Somali and English and lead multi-disciplinary project implementation activities while working under pressure and meeting strict deadlines.
- Proven experience in cybersecurity-related assignments at high-level Government institutions, NGOs, regulatory authorities, international organizations, and various other stakeholders.

5. REPORTING REQUIREMENT

The consultant will report to the client, the National Communications Authority (NCA), through its Director General as a supervisor; the consultant should submit written monthly and quarterly progressive reports with the review and satisfactory approval of the client.

6. DURATION AND LOCATION

The assignment is for a period of twelve (12) months, renewable. The contract may be renewed based on satisfactory performance and availability of project funds. The consultant is expected to be based in Mogadishu, Somalia with possible travel as required by project activities.