Federal Government of Somalia

National Communications Authority (NCA)

TERMS OF REFERENCE (TORs)

FOR

PLAN FOR ESTABLISHING A NATIONAL CIRT AT THE NATIONAL COMMUNICATIONS AUTHORITY (NCA) - FEDERAL REPUBLIC OF SOMALIA

Contents

1. Background 3
2. Objective and Scope 4
   - ❖ Objective 4
   - ❖ Scope of Work 4
   - ❖ Conformity with internationally recognized standards and good practices 5
3. Deliverables 6
   - ❖ List of deliverables 6
   - ❖ Format of Deliverables 7
4. Assignment Duration, Deliverables, and Payment Schedule 7
5. Assumptions 7
6. Consultant Requirements and Qualifications 8
   - ❖ Requirements and Qualification of the Consultant 8
   - ❖ Qualifications of the Consultant's Team 8

ANNEX A – Stakeholders to be included in consultation workshops. 10

ANNEX B - Recognized good practices for establishing CIRTs. 11

1. Background

The National Communications Authority (NCA) is the regulatory body for the communications sector in Somalia. NCA was established through the Communications Act of 2017, and its mandate is to regulate the Communications sector, including telecommunications, Internet, broadcasting, Information and Communications Technology, and e-Commerce services. The NCA is responsible for facilitating the development of the ICT sector, enabling, and ensuring fair and sustainable competition, carrier interconnection, transparency in implementing the Communications Law, protecting consumer interests and rights, and maintaining its role as an independent regulator[1].

Furthermore, the Ministry of Communications and Technology (MoCT) is the lead Federal Government body mandated to formulate national policies, laws, and regulations related to telecommunications and Information and Communications Technology (ICT)[2]. The MoCT developed a 5-year of National ICT Policy and Strategy (2019-2024). However, one of the main key priorities of the National ICT policy and strategy is: "*Ensuring critical infrastructure is protected - establishing a Cybersecurity and Privacy group to oversee the development and enforcement of national cybersecurity policies and establishing a National Computer Emergency Response Team (CIRT)*."[3]

The Cyber Security Department of NCA is mandated to lead and coordinate the national cyber security response in collaboration with the relevant institutions. Cyber Security Department is also responsible for securing, protecting, monitoring, and defending Somalia's cyberspace and valuable cyber assets, as well as advising and providing guidance to government IT and National Critical Infrastructure providers, businesses, the internet community, and citizens of the current threats and vulnerabilities. The Cyber Security Department is the only official single point of contact for government agencies, Internet Service Providers (ISP), ICT Solutions, Telecom Operators, Small and Medium-Sized Enterprises (SMEs), Critical Infrastructure Providers, Academia, and Citizens, including Child Online Protection (COP) for reporting local cyber incidents. It also works collaboratively with law enforcement, defense, national intelligence, and security agencies to solve the most critical cyber issues at national level[4].

[1] https://nca.gov.so/about-us/
[2] https://moct.gov.so/en/about-us/
[3] https://moct.gov.so/en/wp-content/uploads/2019/11/National-ICT-Policy-Strategy-2019-2024.pdf
[4] https://nca.gov.so/cybersecurity/

NCA and MoCT conducted the first National Cyber Security Assessment nationwide between December 2019 - February 2020, in collaboration with the Cybersecurity Capacity Centre for Southern Africa (C3SA), University of Cape Town, and Global Cyber Security Capacity Centre (GCSCC), University of Oxford. The assessment was conducted using Cybersecurity Capacity Maturity Model (CMM) for Nations developed by GCSCC[5].

2. Objective and Scope

❖ Objective

The National Communications Authority (NCA) of Somalia intends to engage a firm ("the Consultant") to develop a National CIRT establishment plan ("the Plan"). The Plan will reflect the needs, requirements, and objectives of the country and will detail the services the national CIRT should provide its target audience and necessary resources. The Plan should also include a step-by-step roadmap for establishing a national CIRT, as well as relevant bidding documentation.

The Consultant will incorporate widely accepted Good Practices to enable national CIRT established through the Plan to participate in international cooperation initiatives and fora (e.g., FIRST). To reach this objective the National Communications Authority (NCA) of Somalia is seeking a firm with a strong track-record in establishing CIRTs, particularly in developing countries.

❖ Scope of Work

The deliverables of this assignment would be notably used to favor the establishment of National CIRT at the National Communications Authority (NCA) of Somalia. The consultant is expected to perform the following tasks:

1. **Desk Research and Preparation for on-site assessment**: The consultant will conduct studies and analysis of the country's current incident response capabilities as well as the broader cybersecurity status. Relevant data and documents can be requested from

[5] https://gcscc.ox.ac.uk/cmm-reviews

the National Communications Authority (NCA) of Somalia or consulted through desk research if available. This task includes the preparation of a list of relevant stakeholders to be interviewed during the consultation workshops.

2. **Conduct consultation workshops with relevant national and regional stakeholders**: The consultant will hold a series of interactions and discussions with relevant stakeholders to assess the level of readiness for the creation of a national CIRT. In this activity, the consultant will conduct interviews, ask about the needs, and discuss existing gaps and possible remediation. This task will inform tasks 3 and 4.

3. **Draft Readiness Assessment Report:** The consultant will prepare a report based on the information collected in Tasks 1 and 2. The report will provide an overview of the existing incident response capabilities in the country, outlining preliminary requirements (e.g., mandate, governance, high-level roadmap, budget) for the National CIRT establishment plan, and provide insights on the broader cybersecurity context.

4. **Draft National CIRT Establishment Plan**: The consultant will develop a comprehensive plan that defines the services, target audience, necessary resources, and other relevant elements for establishing a national CIRT in the country. The consultant will also provide a step-by-step roadmap for implementing the plan.

5. **Reporting to Project Manager:** The consultant will report regularly to the project manager and provide Status Update Reports, presentations, and other forms of communication as required.

6. **Other Applicable Tasks**: The consultant will carry out any additional tasks requested by the project manager within the scope of the deliverables outlined in this ToR.

❖ Conformity with internationally recognized standards and good practices

All the activities and deliverables mentioned in this ToR shall be completed in conformity with the main internationally recognized standards and good practices. Annex B reports an indicative list of resources.

3. Deliverables

❖ List of deliverables

The consultant is expected to produce the following four (4) deliverables:

- **Deliverable 1: Inception report including work plan and schedule.**
- **Deliverable 2: Consultation workshop with national and regional stakeholders (up to 5 days).** The National Communications Authority (NCA) will support the organization of the workshops. The list of national and regional stakeholders that will participate in the workshop will be agreed upon with NCA. Annex A provides a list and a rationale of stakeholders that should be considered to participate in the workshop.
- **Deliverable 3: Readiness Assessment Report**. This report shall include, among others, the following elements:
    - ❖ Brief review of existing incident response capabilities.
    - ❖ Preliminary Mandate.
    - ❖ Governance Structure.
    - ❖ Requirement for CIRT hosting organization.
    - ❖ High-level roadmap and budget.
    - ❖ High-level requirements for the Design Stage.
- **Deliverable 4: CIRT Establishment Plan**. The Plan shall include, among others, the following:
    - ❖ Detailed Mandate
    - ❖ CIRT Services Plan
    - ❖ CIRT Processes and Workflows Plan
    - ❖ CIRT Organization, Skills, and Training Structure Plan
    - ❖ CIRT Facilities Plan
    - ❖ CIRT Technologies and Processes Automation Plan
    - ❖ CIRT Cooperation Plan
    - ❖ CIRT IT and Information Security Management Plan
    - ❖ Detailed roadmap and Requirements for the Implementation Stage
    - ❖ Bidding documentation (e.g., Terms of Reference) to establish the CIRT

❖ Format of Deliverables

Deliverables 1, 3, and 4 will be delivered in the form of documents (e.g., Excel, Word, PowerPoint; etc.). Deliverable 2 will be delivered in the format of up to 5 days of the on-site or virtual workshop.

4. Assignment Duration, Deliverables, and Payment Schedule

The estimated duration of this assignment is **Eight (12) weeks**, beginning on **01 August 2023, and** ending on **31 October 2023**. The completion of the deliverables should follow the timeframe outlined below:

#	Deliverables	Timeline	Payment Schedule
1	**Deliverable 1**: Inception Report including work plan and schedule	Week 1	10%
3	**Deliverable 2**: Consultation workshop with national and regional stakeholders (up to 5 days)	Week 3	25%
4	**Deliverable 3**: Readiness Assessment Report	Weeks 7	25%
5	**Deliverable 4**: CIRT Establishment Plan	Weeks 12	40%

Vendors are invited to suggest alternative timelines in their proposals.

5. Assumptions

- The Consultant will not perform any intrusive or technical assessment at a client site.
- The deliverables procured through this engagement are advisory in nature. The National Communications Authority (NCA) will appoint a qualified person to play the role of Engagement Manager to oversee the engagement.
- The National Communications Authority (NCA) will provide to the consultant with relevant documents such as policy, strategies, risk assessments, and other relevant data and information that could help the Consultant deliver the expected outcomes. National

Communications Authority (NCA) will make subject matter experts available for interviews and information gathering.

- The National Communications Authority (NCA) will provide help to identify the list of stakeholders and preparatory documentation for interviews in a timely manner.
- The National Communications Authority (NCA) will have three **(2) weeks** to review and provide feedback for each deliverable.
- The National Communications Authority (NCA) will be responsible for all management decisions relating to the engagement and resulting deliverables, the use or implementation of the output of the engagement, and for determining whether the deliverables are appropriate for their purposes.
- The National Communications Authority (NCA) will own the intellectual property rights of the deliverables created through this engagement.

6. Consultant Requirements and Qualifications

❖ Requirements and Qualification of the Consultant

The Consultant shall comply with the following experience and qualifications. The consultant will be recruited on a competitive basis in accordance with the World Bank procurement guidelines.

- At least 7 years of experience in cybersecurity, specifically incident response, cyber threat intelligence, and digital forensics.
- At least 3 project references in the past 5 years of assessing, establishing/enhancement of national/sectorial CIRT/CSIRT/SOC. Reference letters signed by the customer must be provided with the proposal.
- At least five years of experience with:
    - Integrating and customization of CIRT/CSIRT/SOC Tools.
    - Developing policies and procedures related to CIRT/CSIRT/SOC operations (operational workflows, SOPs, incident management processes, service level management frameworks, among others).
    - Setting up Cybersecurity Operation Center tools; configuring honeypots and integrate external feeds, setting up digital forensic solutions.
- Previous projects in the region are a plus.

❖ Qualifications of the Consultant's Team

The Consultant's team should be composed of at least the following members:

Team Leader (1)

- University bachelor's or master's degree in computer science, IT, engineering, or a related field.
- At least seven (7) years of experience in a Cybersecurity program or project management experience specifically incident response, cyber threat intelligence, and digital forensics.
- Proven experience in managing and implementing CIRT/CSIRT/SOC related projects in developing countries would be an advantage.
- Relevant CIRTifications such as CISSP, CISM, or GCIH and internationally recognized SOC auditor CIRTification.
- Fluency in English.

Project Team Members (3)

- At least five years of experience in cybersecurity specifically incident response, cyber threat intelligence, and digital forensics.
- Proven work experience in implementing CIRT/CSIRT/SOC related projects in developing countries would be an advantage.
- Relevant CIRTifications such as CISSP, CISM, or GCIH and internationally recognized SOC auditor CIRTification.
- At least one project team member should be CIRTified EnCase CIRTified Examiner (EnCE) and/or EnCase CIRTified eDiscovery Practitioner (EnCEP).
- At least one project team member should be a CIRTified Cellebrite CIRTified Mobile Examiner (CCME).
- Fluency in English.

ANNEX A – Stakeholders to be included in consultation workshops.

- Relevant Ministries representatives.
- Policy Makers (parliamentarians).
- Judiciary System.
- Regulatory Bodies.
- National Security Agencies.
- Military Establishment (or those currently responsible for information security and/or IT and ICT management).
- Law Enforcement Agencies.
- Critical Infrastructure Providers (Water, Energy, Transport, etc.).
- Central Monetary Agency and Banks (most relevant public and commercial).
- Telecommunication Operators and Internet Service Providers.
- Academia and National Research Bodies.
- Local Industry (Private Sector) involved in security initiatives.

ANNEX B - Recognized good practices for establishing CIRTs.

- Carnegie Mellon University, 2016, *Create a CSIRT*, Software Engineering Institute, Pittsburgh, PA. Cowley, C. and Pescatore, J., 2019, *Common and best practices for security operations centers: Results of the 2019 SOC survey*, SANS Institute. ENISA, 2006, *A step-by-step approach on how to set up a CSIRT*. https://www.enisa.europa.eu/publications/csirt-setting-up-guide
- FIRST, 2019, *Computer Security Incident Response Team (CSIRT) Services Framework* https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1
- IETF Internet Engineering Task Force, 1998, RFC 2350 for CSIRT establishments. https://tools.ietf.org/html/rfc2350
- Internet Governance Forum, 2014, Best practice forum on establishing and supporting computer security incident response teams (CSIRTs) for internet security https://www.intgovforum.org/multilingual/content/establishing-and-supporting-computer-incident-security-response-teams-csirts-for-internet.
- MITRE, 2014, *Ten strategies of a world-class cybersecurity operations center*, MITRE, Bedford, MA.
- Morgus, R., Skierka, I., Hohmann, M. and Maurer, T., 2015, *National CSIRTs and their role in computer security incident response*, New America and GPPi. https://www.researchgate.net/publication/323358191_National_CSIRTs_and_Their_Role_in_Computer_Security_Incident_Response
- National Cyber Security Centre, 2015, *CSIRT Maturity Kit*, National Cyber Security Centre, the Hague.
- National Cyber Security Centre, 2017, *Building a SOC: Start Small*, National Cybersecurity Centre, the Hague.
- Organization of American States, 2016, *Best Practices for Establishing a National CSIRT*, OAS, Washington, D.C.
- Open CSIRT Foundation, 2008-2019, SIM3: Security Incident Management Maturity Model. https://opencsirt.org/csirt-maturity/sim3-and-references/
- Skierka, I., Morgus, R., Hohmann, M. and Maurer, T., 2015, *CSIRT Basics for Policy-makers*, New America and GPPi. (https://www.researchgate.net/publication/323358187_CSIRT_Basics_for_Policy-Makers)

- Telecommunications Development Sector (ITU-D), 2020, ITU CIRT framework, International Telecommunication Union, Geneva.
- ThaiCIRT, 2017, *Establishing a CSIRT*, Thailand Computer Emergency Response Team, Bangkok.
- TNO, 2017, *GFCE global good practices: National computer security incident response teams (CSIRTs)*. (https://thegfce.org/wp-content/uploads/2020/06/NationalComputerSecurityIncidentResponseTeamsCSIRTs-1.pdf)