República Democrática de São Tomé e Príncipe

(UNIDADE – DISCIPLINA – TRABALHO)

Ministério das Infraestruturas, Recursos Naturais e Meio Ambiente

PROJETO STP DIGITAL

Terms of Reference

Establishment of the Sao Tome and Principe National Computer Security Incident Response Team (CSIRT)

---

1. Background

The Government of Sao Tome and Principe (the Government) supported by the World Bank is undertaking an investment program under the Digital Sao Tome and Principe (STP) project to strengthen its ICT sector. This will include investment in telecommunications infrastructure, foundational digital government platforms, cybersecurity, and improvement of connectivity to schools.

Currently, the Government's cybersecurity capacity is nascent, with no national legislation or strategy for cybersecurity in place. However, a separate engagement is currently underway to develop the National Cybersecurity Strategy and associated Action Plan, for completion later in 2023.

A key component of the cybersecurity strategy is the establishment of a the National CSIRT. Currently, the Government does not have the operational capacity to mitigate cybersecurity risk or threats, with no CSIRT or similar function in place. The Digital STP project includes funding for the creation and operationalization of the National CSIRT agency.

2. Objective

The objective of this assignment is to support the Government to design, establish and operationalize a CSIRT function either within an existing institution or ministry, or as a separate agency within Government.

The CSIRT will have the following responsibilities:

- Serve as a trusted focal point of contact and coordination within and beyond national borders;
- Identify and manage cyber threats that may have adverse effect on the country;
- Help systematically respond to cyber security incidents and takes appropriate actions;
- Help the constituency to recover quickly and efficiently from security incidents;
- Minimise loss or theft of information and disruption of services;
- Establish and nurture relationships with other international/regional CSIRTs;
- Make general security best practices and guidance available through publications, websites, and other modes of communications; and

- Participate in initiatives (or set directions and drive the projects) pertaining to developing national policies, strategies, laws and regulations for cybersecurity.

The assignment will have multiple components, including the drafting of policies, regulations, standards, and guidelines. It will also propose a structure for the CSIRT that is technically, financially, and operationally sustainable for a small government system such as in Sao Tome and Principe; support the Government in standing up and operationalizing that structure; provide trainings for the CSIRT personnel; and assist the CSIRT to establish relationships with other international/regional CSIRTs.

3. Scope of Work

The assignment will be split into three phases; the *Planning Phase*, the *Implementation Phase*, and *Operational Support Phase*. It is expected that the total timeframe for this engagement will be 3 years, with the first two years spent on Phase 1 and 2 (Planning and Implementation), and the final year on Phase 3 (Operational Support).

Phase 1: Planning

The Planning Phase will focus on the development of policy and organizational and operational planning for the CSIRT. It will include all activities needed to develop and obtain approval for the full CSIRT establishment plan. This will include, but not be limited to, the following:

- Evaluation and assessment of any legal and policy changes required in Sao Tome and Principe to institutionalize the CSIRT, noting the Government is also in parallel developing the National Cybersecurity Strategy which will call for a CSIRT;
- Consult with relevant Ministries and assess the institutional mandate of technical agencies (such as AGER, INIC), in order to determine the agency in charge of coordinating the CSIRT and to obtain Government approval. This activity should take in consideration results from institutional assessment and consultations that took place for the development of the National Cybersecurity Strategy.
- Development of overarching principles, roles and responsibilities for the design of the CSIRT, taking into account the small size of the Sao Tome and Principe system and the cybersecurity risk landscape specific to the country context;
- Development of organizational structure aligned with the specific needs of the country. This will include both operational and management resources required, as well as the proposed governance structure for the CSIRT;

- Development of relevant operating processes and procedures for the CSIRT when operational, utilizing appropriate international best practice guidelines or standards such as ISO27002 where applicable, and ensuring that they are fit for purpose for the small size of the CSIRT proposed;
- Design and evaluation of proposed operational toolsets and platforms to be utilized by the CSIRT;
- Development of full establishment project plan, highlighting all relevant activities to establish the CSIRT along with associated timeframes and resource requirements;
- Development of a financial plan and budget for both the implementation and annual operating costs of the CSIRT;
- Support to seek approval of the CSIRT Establishment Plan by relevant stakeholders within Government, include the regulator AGER and the Ministry of Infrastructure and Natural Resources (MINR).

Phase 2: Implementation

The Implementation Phase will focus on the activities required to set up and operationalize the CSIRT, based on the approved Establishment Plan. This will include, but not be limited to, the following:

- Project management of the CSIRT Establishment Plan and all associated activities;
- Support to the Government to institute the agreed organizational structure and to recruit and staff the required resources;
- Support to the CSIRT staff to stand up operational processes and procedures, including reporting mechanisms;
- Provision of training to CSIRT management and operational staff to improve skill sets, knowledge and competency in CSIRT operational processes;
- Support to the Government to procure, configure and operationalize relevant CSIRT toolsets and technical platforms;
- Support to develop appropriate intellectual property for the CSIRT, including initial online presence and cybersecurity awareness campaign material.

Phase 3: Operational Support

The Operational Support Phase will focus on providing 12 months of operational support to the new CSIRT, including providing additional training, simulation and support for CSIRT operations such as incident response, awareness campaigning and risk/vulnerability monitoring. This will include, but not be limited to, the following activities:

- Ongoing training and simulations in CSIRT operational activities to provide continuous improvement of CSIRT operations;

- Review and improvement of CSIRT processes and procedures as the CSIRT matures once operational;
- Support to launch initial awareness campaigns and conduct public outreach activities
- Ad hoc support and advice to operational risk management and incident response activities to help the CSIRT capability carry out its initial operational responsibilities.

4. Reporting and Time Schedules

Due to the long timeframe of the engagement, time frames set out below are provisional only and can be negotiated following the development of the appropriate project plans for each phase as the assignment progresses.

Phase	Item	Deliverable	Timing	Payment
1	1	Contract signature	Contract Signature	
	2	Inception report describing the approach and methodology that will be used for supporting the development of the CSIRT Establishment Plan, including a project plan, the proposed governance committees and a stakeholder engagement plan, including a list of stakeholders for consultation	Contract Signature + 1 month	10%
	3	Legal and Policy Assessment, and development of principles for CSIRT design	Contract Signature + 3 months	5%
	4	Draft CSIRT Establishment Plan, including implementation phase project plan, financial plan, proposed organizational structure	Contract Signature + 6 months	5%
	5	Second Draft CSIRT Establishment Plan, with additional sections including process and procedure design, and proposed toolset and platform requirements	Contract Signature + 9 months	5%

	6	Final CSIRT Establishment Plan following consultation with stakeholders and approval from Government to continue to Phase 2	Contract Signature + 12 months	15%
2	7	CSIRT organizational structure and resources in place	Start of Phase 2 + 6 months	10%
	8	CSIRT training delivered; processes and procedures documented; pilot phase concluded and CSIRT operational	Start of Phase 2 + 12 months	20%
3	9	Phase 3 Milestone 1: training, process improvement review and ad hoc operational support delivered	Start of Phase 3 + 6 months	10%
	10	Phase 3 Milestone 2: training, process improvement review and ad hoc operational support delivered	Start of Phase 3 + 12 months	20%

5. Procurement Approach

Commencement of subsequent phases following Phase 1 will be dependent on suitable performance in the previous phase, and the purchaser reserves the right not to continue the contract into the following phase should performance requirements not be met.

All technical toolsets and platforms will be procured separately to this assignment, in line with Government and World Bank procurements rules, and are not included in scope of this terms of reference.

6. Qualification, Experience and Language

The selected firm should display the following capabilities:

- Extensive knowledge of cybersecurity policy, strategy and operations in a government context;
- Leading information security organization with experience of rolling out similar CSIRT establishment programs at the national level in at least two countries, with small country system experience an advantage;

- Demonstrated capability in design, development and delivery of information security policies, regulations, standards and guidelines as evidenced by the qualifications and experience of professional staff;
- At least 5 years of experience in conducting similar consultancies
- Should have strong partnerships with CSIRTs and Cyber Security Centers in other countries

The team shall propose a team comprising a Team Leader, a team of specialists with relevant experience and qualifications and other support staff as they feel fit for the exercise.

Team Leader

- At least master's degree in related subjects with minimum of 8 years' experience in a leadership role in designing and setting up national CSIRTs in at least two countries. The team leader should have EC Council/SANS/ CISSP/Equivalent Certification.
- Experience in Sub-Saharan Africa or in SIDS especially in Sao Tome and Principe is desirable.

Expert in CSIRT Design and Operations

- At least master's degree in related subjects minimum 5 years' experience structuring and setting up CSIRTs. Experience in providing CSIRT specific training and developing financial and operations plans in at least two countries.
- All key experts mentioned above must have international experience (one country outside their home country).

For all other specialist team members other than support staff, at least 10 years' experience is required with relevant experience of their field in an African setting. CVs of the proposed non-key professional staff should be provided.

The language requirement is Portuguese in Sao Tome and Principe. English is suitable, but the successful firm must provide interpretation services for meetings and translation services for documents should their primary language not be Portuguese. All training, documents and studies should be delivered in Portuguese.

7. Counterpart Facilities

The project will provide institutional support and all available documents, data and information to the consultant. The consultant should include all eligible expenditure in the financial proposal for accommodation, logistics and required manpower for successful implementation of the assignment.

8. Duration:

This activity shall be implemented over three (3) years in the assigned phases. Timing of the individual phases is flexible within this period, according to needs and delivery requirements.