Terms of Reference (TOR)

Assignment Title: Development of Critical Information Infrastructure Protection Capacities
Country: Independent State of Samoa
Project Name: Digitally Connected and Resilient Samoa Project
Project ID: P180807
Duration of the assignment: 24 months

Project Background

The Government of Samoa (GoS) recognizes the importance of ensuring an enabling and secure environment for digital transformation as reflected in key national strategic planning documents such as the Pathway for the Development of Samoa (PDS) FY2021/22–FY2025/26, the pending Samoa Digital Transformation Strategy 2023 – 2030 and Samoa National Cybersecurity Strategy 2025-2030, and the ICT Sector Plan FY2022/23 – 2027/28.

The GoS has received financing from the World Bank for the Digitally Connected and Resilient Samoa Project (DCRSP), which seeks, inter alia, to enhance the capacity of the GoS to deliver digitally enabled, inclusive, secure and safe public services. The Project will focus on digital connectivity and digital government infrastructure, including an upgrade and extension of Samoa's national fiber network, alongside measures to enhance cybersecurity resilience and safeguard the reliability of essential digital services.

The DCRSP will support significant investments in information technology infrastructure as part of the GoS broader strategy in working towards the sustainable development of Samoa in relation to economic performance; to productivity, effectiveness and efficiency in the public and private sectors; to quality education and health services; and to civil society inclusive of people with disabilities. This project will also support the Samoa National Computer Emergency Response Team (SamCERT) to enhance cybersecurity governance, improve incident response capabilities and promote online safety for citizens. These efforts will help Samoa move towards its goal of a fully realized digital ecosystem, which can help foster inclusive growth and improve the quality of life for all Samoans.

The Project comprises of three (3) main components:

i) Digital Connectivity and Digital Government Infrastructure

ii) Strengthening and enhancing the enabling environment for digital transformation

iii) Project Implementation Support

This assignment falls under Component 2, specifically Sub-component 2.3b of the Project which supports the establishment of Critical Information Infrastructure Protection (CIIP) Capacities. The Ministry of Communications and Information Technology (MCIT) is the lead Implementing Agency (IA) for this sub-component.

Assignment Background

The transformation supported by digital infrastructure developments and increasing demand for digital services requires that adequate safeguards and security measures be in place to ensure continuity of critical services in the event of any potential disruption. This is crucial, especially for essential services supported and enabled by digital technology.
Critical Information Infrastructures (CIIs)—including systems in sectors such as energy, finance, telecommunications, transport, health, and water—are essential to the functioning, security, and socio-economic stability of Samoa. Increasing digitalization has expanded the cyber threat landscape, making these infrastructures attractive targets for cyberattacks, such as ransomware, supply-chain compromises, often perpetrated by Advanced Persistent Threats

(APT) groups. While some issues are the result of deliberate cyber threats, the growing reliance on digital infrastructure also creates vulnerabilities stemming from system shortcomings or failures. To strengthen national resilience, there is a need to enhance Samoa's Critical Information Infrastructure Protection (CIIP) capacities. Hence, the MCIT seeks to engage a qualified consultancy firm to support the development of the CIIP capacities through framework development, training, and institutional strengthening.

This Terms of Reference (TOR) sets out the conditions of the proposed assignment requiring the technical assistance of a consultancy firm ('Consultant') to assist the Government of Samoa in the development of Critical Information Infrastructure Protection Capacities.

Objective of the assignment:

An international firm is sought to assist the GoS in providing technical assistance to support the development of CIIP capacities as well as timely, responsive and appropriate outputs across the various phases stipulated below:

1. Development of CIIP (Governance) Framework and identification of CII
2. Development of CIIP Guidelines
3. Support the Implementation and Supervision Mechanisms

Scope of Services

A key focus of the firm will be to design, establish, and operationalize Samoa's Critical Information Infrastructure Protection (CIIP) capacities through a structured, phased approach that addresses governance, legal and institutional frameworks, identification of CIIs, practical guidelines for operators, and mechanisms for implementation, supervision, and capacity building.

Given that Samoa is a small nation with limited resources and institutional capacity, the CIIP development process should emphasize simplicity, sustainability, and streamlined procedures. The Consultant is expected to tailor the proposed frameworks, guidelines, and tools to Samoa's context by prioritizing practical, easy-to-implement solutions derived from the core elements of international standards, rather than adopting overly complex or resource-intensive models.

The firm will assist the Government in performing the following specific activities:

Phase One - Development of CIIP (Governance) Framework and Identification of CII

(Estimated Timeframe: 6-9 months)

This component will create the overarching foundation for Samoa's CIIP, by defining the scope, governance, and institutional arrangements, and providing the methodology and tools necessary for identifying and designating CIIs and implementing the CIIP guidelines. This phase will conclude with the delivery of the CIIP Framework Handbook - which will set out the strategic, institutional, legal, and operational principles of CIIP - and a CII identification process that will support the formal designation of Samoa's CII list.

The CIIP Framework Handbook will cover the following key Elements:

- **Define the Scope and Objectives** - The Consultant shall articulate the purpose, scope, and guiding principles of the national CIIP framework. This work must align with the drafted National Cybersecurity Strategy (NCS) 2025–2030, the Information Security (IS) Policy 2024, and broader national priorities. Deliverables should clearly

describe how the CIIP supports national resilience, security, and digital transformation objectives.

- **Develop the CIIP Governance Model** – The Consultant shall design the institutional architecture, roles, and responsibilities for CIIP governance, including coordination mechanisms between government, regulators, CII operators, and other stakeholders.
- **Identify Participating Stakeholders and Institutional Roles** – The Consultant shall map all relevant public and private stakeholders and specify their respective roles and responsibilities (governance, oversight and operational) in the CIIP ecosystem. This should all be clearly outlined in a Stakeholder Engagement Plan which covers the duration of the assignment.
- **Define the Key Domains of the CIIP Guidelines** – The Consultant shall identify and structure the substantive domains to be included in the CIIP guidelines, such as organizational (e.g., staffing, certifications, management involvement, etc.), operational-procedural (e.g., incident reporting, business continuity), technical (e.g., access control, penetration testing) and physical.
- **Develop the Compliance Framework and Enforcement Mechanisms** – The Consultant shall propose a framework for monitoring, assessing and enforcing compliance, including reporting obligations, incentives and penalties. The Consultant should review the existing IS Policy audit plan and ensure that the compliance framework is aligned with and builds upon it, using the current audit mechanisms as a baseline and extending them to address CII-specific requirements.
- **Assess Legal Mandates** – The Consultant shall review the existing legal and regulatory framework to identify necessary amendments that will enable the effective monitoring and enforcement of CIIP obligations. These required amendments should be integrated into the broader DCRS legislative review of ICT laws. A mechanism to discuss and coordinate these alignments will be established with the DCRS-designated legal team. The Consultant should familiarize with existing GOS requirements relevant to the Project as outlined in the Cabinet Handbook 2011 and as per the Environmental and Social Safeguards (ESS) 10 – Stakeholder Engagement & Information Disclosure of the World Bank's Environmental and Social Framework (ESF)
- **Develop the CII Identification and Designation Procedure** – The Consultant shall design a practical, scalable, and repeatable method for identifying and designating CIIs. This procedure should include clear criteria for assessing essential services and CII operators, suitable for environments where detailed quantitative data may be limited. The Consultant shall outline a step-by-step process that can be operationalized by national authorities.

The development of the CIIP Framework Handbook will be conducted through sector-level consultation and collection and analysis of sectoral information on essential services. The CII Identification Procedure will guide a structured consultation effort aimed at mapping essential services and their operators, assessing the potential impact of disruption, and determining

appropriate thresholds for designation. This exercise will result in a formal list of CIIs, submitted for government approval.

Phase Two - Development of CIIP Guidelines

(Estimated Timeframe: 4-6 months)

This phase will translate the strategic and governance principles of the CIIP Framework into concrete, actionable operational requirements for CII operators, and will be concluded with the submission of a CIIP Guidelines Handbook.

The CIIP Guidelines Handbook will set out specific organizational, procedural, technical, legal, managerial, and physical protection measures to be adopted by the designated CIIs. The guidelines must be clear, actionable, and tailored to Samoa's national context and institutional capacities, while drawing from international good practices and standards.

To simplify the development of the CIIP Guidelines, the Consultant is expected to use Samoa's IS Policy 2024, as the starting point. The Consultant should review the IS Policy and propose how it can be leveraged to form the core of the CIIP Guidelines, identifying where additional CIIP-specific provisions are necessary.

The Consultant is also expected to benchmark international good practices (e.g., EU NIS2, NIST CSF, ISO 27001/27019, sector-specific standards), assess Samoa's existing environment, and suggest a pragmatic customization approach.

The development of the CIIP Guidelines Handbook will be conducted through stakeholder consultations and validation, including regulators and identified CIIs, to confirm that the proposed CIIP requirements are feasible and well understood.

Phase Three - Implementation and Supervision

This phase will translate the CIIP Framework and CIIP Guidelines into practice by ensuring that designated CIIs have the capabilities, resources, and support necessary for effective implementation.

The focus will be on assessing national and sectoral readiness, defining the practical steps for operationalizing CIIP requirements, and initiating capacity-building and rollout activities.

This phase is intended to establish a sustainable foundation for ongoing CIIP compliance monitoring, and continuous improvement.

The Consultant is expected to undertake the following tasks:

- Capacity and Expertise Requirements – Assess the skills, knowledge, and technical capabilities needed for CIIP implementation in SamCERT and across CIIs.
- Technical Tools and Security Measures – Identify the essential systems, tools, platforms, and technologies required to enable the adoption of the CIIP guidelines in SamCERT and across CIIs.
- Development of the implementation plan by defining steps, timelines, responsibilities, and resource needs (skilled manpower and technical tools and systems), for rolling out the CIIP Guidelines to all designated CIIs.
- Implementation Kickoff with the rollout of introductory workshops and capacity building programs.

Please note that following the introductory workshops, SamCERT will support the soft implementation process across CIIs. SamCERT will support initial adoption through phased rollout to identify gaps, provide advice and support, and allow operators to adapt before full enforcement.

- Establishment and testing of compliance monitoring processes, including audits, reporting systems, and periodic reviews.

Deliverables, Timing, and Administrative Arrangements

The Consultant will submit deliverables according to the following schedule summary and initial timing assumptions:

Deliverable	Description	Completion date	Payment Schedule
Phase 1 – 35%			
1.1 Inception Report	The Inception Report provides information and clarity on assignment management and governance, execution methodology, communication channels, and approval processes. It discusses the risks, proposes mitigations, and sets up a clear timeline for implementation with a list of tasks and deliverables. In addition, given the highly consultative nature of this assignment a stakeholder engagement plan is a necessary component of the inception report.	2 weeks after contract signature	10%
1.2 CII Framework Handbook	A long-term reference point for the development, implementation, and governance of CIIP in the country. This framework will define the strategic, institutional, legal, and operational principles of CIIP. It will set out the scope, objectives, governance model, technical and capacity requirements, and the full range of substantive areas that should be covered by the CIIP guidelines.	6 months after contract signature	15%
1.3 CII Identification Procedure	The CIIP Identification Procedure will define the criteria, and processes for systematically identifying and designating Critical Information Infrastructures in Samoa. Considering Samoa's size, the procedure will be simple and straightforward.	6 months after contract signature	5%
1.4 Proposed list of designated CIIs	Using the developed procedure, guide the identification process to produce a proposed list of Samoa's CIIs, including justification for each designation.	9 months after contract signature	5%
Phase 2 – 15%			
2.1 CIIP Guidelines Handbook	Guidelines for CII - including a list of provisions, procedures, thresholds and minimum requirements	12 months after contract signature	15%
Phase 3 – 50%			
3.1 CIIP Introductory Workshops	Support the delivery of CIIP Guidelines introductory workshops, training sessions,	12 months after	10%

	and supporting materials to SamCERT, designated CIIs and relevant stakeholders.	contract signature	
3.2 CIIP Compliance Assessment	Individual reports produced for each designated CII that undergoes an audit, documenting findings, compliance levels, and recommended corrective actions.	18 months after contract signature	20%
3.3 CIIP Implementation Plan	A detailed plan covering timing, resources, roles and responsibilities, required capacity-building activities, soft implementation arrangements, and audit/monitoring plans.	18 months after contract signature	15%
3.4 Implementation Support and Progress Report	A report tracking the progress of CIIP implementation, capturing the outcomes of the soft implementation process, and assessing the overall level of compliance among CIIs.	24 months after contract signature	5%

Expected Outcomes

The assignment will be paid on a lump sum basis at the specified schedule agreed with the consultancy firm on the completion and acceptance of deliverables as set out in Schedule. The amount of time required for tasks will be agreed with MCIT in writing prior to the commencement of work. The contract period is 24 months from the commencement of this assignment, or such longer period as may be agreed in writing.

Reporting Requirements

The Consultant shall report to MCIT. The form and substance of the reporting will be agreed between the Consultant and MCIT. Any reports required from the Consultant will also be copied in draft and final to the World Bank. The Consultant shall commence work immediately upon the award of the contract. An inception report in the form of a review of the forward-looking project work plan. The inception report shall outline realistic completion dates for Phase 1 and 2 of developing the CIIP capacities, the required key milestones to enable completion within that timeframe, the key activities that will be required to be undertaken by the relevant work stream leads to enable those milestones to be met, and the key risks that will need to be addressed and steps to mitigate those risks. Realistic dates for Phase 3 can be determined at a later stage however a proposed general outline would be ideal. The inception report shall be delivered within two weeks after contract signature, or as otherwise agreed by the Government and the Consultant.

All deliverables shall be provided to MCIT and the World Bank for review before they are finalized and accepted. MCIT and the World Bank agree to respond within a reasonable time frame, which shall generally be no later than 10 working days after submission of the draft, to enable efficient progress of the Consultant's work. Daily supervision and guidance will be provided by the MCIT CEO.

The Consultant shall immediately advise the Government of any direct or indirect financial interest or other enduring professional relationship which might reasonably be seen to affect the impartiality of their advice to the Government under this assignment.

To assist good work planning, budgetary management and transparency, the Consultant shall provide a progress report every two months tracking against workplan.

Initial Reports / Outputs	**Due Date**
Inception report with agreed project workplan review	2 weeks after contract signature
Progress reports to be submitted to the WB, ICT SCD and CEO MCIT every 2 months	5th working day after the end of every 2 months

Selection Criteria

The Consultant must demonstrate proven experience in delivering comparable assignments related to CIIP program design in government contexts. The proposed team should combine both policy, technical and operational expertise.
The Consultant may propose the team composition, including at least:

I. **Team Leader** – The team leader oversees the overall implementation of the assignment and ensures the timely delivery of outputs, methodological consistency, and quality assurance of all deliverables. The team leader will manage coordination with SamCERT and CIIs, lead reporting and workshops, develop implementation plans, and manage risks.
   - **Qualifications:**
     i. Master's degree in Cybersecurity, ICT Management, Project Management, Business Administration, or a related field.
     ii. Certifications such as PMP, PRINCE2, CISSP, or CISM are preferred.
   - **Experience:**
     i. Minimum 10 years of experience managing large-scale cybersecurity or ICT infrastructure projects, including at least one project involving national-level CIIP development.
     ii. Excellent verbal and written communication skills and demonstrated leadership in coordinating multi-stakeholder engagements.
     iii. Experience advising governments or public sector entities preferred.
     iv. Experience coordinating multi-stakeholder engagements.

II. **CIIP and Risk Management experts** – The CIIP experts will lead the substantive technical work required for the development of the CIIP Framework and CIIP Guidelines and will provide technical support throughout the implementation phase across designated CIIs.

Team Qualifications:

The CIIP experts must demonstrate the following qualifications:

- Relevant academic backgrounds in cybersecurity, information security, or related fields.

- Certifications such as CISSP, CISM, ISO 27001 Lead Implementer/Auditor, GIAC or relevant.
- Training or certifications in critical infrastructure protection, cyber risk assessment, or operational technology (OT) security are considered an asset.
- Strong communication and facilitation skills for stakeholder engagement and training.

Experience

- At least 7-9 years of experience in CIIP, cybersecurity policy, cyber resilience, or related fields.
- Experience conducting national-level cybersecurity assessments or CIIP projects.
- Proven experience in CIIP planning, frameworks, CERT operations, or cyber exercises.
- Demonstrated expertise in risk assessment, incident response, and CII governance.
- Experience facilitating technical workshops, consultations, or capacity-building sessions with government agencies, regulators, and operators.
- Stakeholder Strategy, Planning and Execution - A moderate experience in and/or demonstrates a proficiency level enough to lead the planning, development and execution of a stakeholder strategy in support of the defined objectives.

In addition to the mandatory requirements, the following are skills / experience desirable

- Successful completion of at least 3–5 similar projects for governments, donors, or critical sectors.
- The Consultant shall also have worked directly for Government(s) at the highest levels and held strategic and policy responsibilities for issues of national significance and visibility;
- Previous experience advising on public sector infrastructure or digital transformation projects and experience working for government stakeholders in the Pacific region or in countries with similar institutional and sectoral contexts is essential. Specific experience working on similar assignments in Samoa is an advantage;
- Demonstrated ability to work successfully with project team members, governments, regulatory bodies, local communities and other stakeholders.

Client's Inputs

The Client shall provide office space, internet connection and print facilities when the Firm is in Samoa.

Duration of assignment

The assignment is expected to be completed over a period of 24 months.