Government of Tonga-Ministry of Finance

REQUEST FOR EXPRESSIONS OF INTEREST

CONSULTING SERVICES – FIRM SELECTION (International)

Assignment Title: Cyber security Consultancy Services (Consulting Firm) for developing and supporting information systems

Project: Tonga Digital Government Support Project.

Grant Number: IDA Grant Number **IDA D4490-TO**

Date of Issuance: 11th October 2019.

Date and time Expression of Interest (EOI) due: 8th November 2019. No later than 4:30 pm local time

Drop off EOI to Main Office: Ministry of Finance, Nuku'alofa, Tonga

Email Submission of EOI: Please email to: ***bfaotusia@finance.gov.to*** and copy to ***qfukofuka@finance.gov.to*** *and to* ***npelesikoti@finance.gov.to***

Attn: Chief Executive Officer, Ministry of Finance

Reference Number: TO-MFNP-128783-CS-CQS

The Government of Tonga has received financing from the World Bank toward the cost of the Tonga Digital Government Support Project (TDGSP) and intends to apply part of the proceeds for consulting services.

The consulting services ("the Services") include the recruitment of the Cyber security firm that will be responsible of the following: (i) Lead the Tonga Cybersecurity Program, including development and management of Cybersecurity services, and products; (ii) Develop Tonga Cybersecurity standards, adopting international government and generic (ISO) standards applicable to the Tonga government, business, and public environment; (iii) Manage development and delivery of ongoing program components; (iv) Develop initial and recurring Cybersecurity training and awareness program for all government employees; (v) Develop minimum Cybersecurity skills and certification requirements for Tonga network, software development, and information systems management staff; (vi) Establish and manage Cybersecurity Program Office; and (vii)Transfer knowledge and build capacity of permanent Government staff

The duration of the assignment is over a period of 18 months.

The detailed Terms of Reference (TOR) for the assignment are shown in Annex 1.

The Ministry of Finance as the Implementing Agency for Tonga Digital Government Support Project now invites eligible consulting firms ("Consultants") to indicate their interest in providing the Services. Interested Consultants should provide information demonstrating that they have the required qualifications and relevant experience to perform the Services.

Minimum Qualification and Experience Requirements

The Consulting Firm

The following minimum qualifications and experience are required and will be used to evaluate the potential consultants (consulting firms). The consulting firm should be qualified and experienced for carrying out this assignment. The firm should demonstrate at least 10 years of experience in similar services and at least 3 contracts of similar assignments successfully performed for the last five (5) years. The consultant will propose a team of Experts that will include the following specializations:

Team Leader (1)

Qualifications and Experience

- Required - Degree in electrical engineering, systems engineering, computer science, computer engineering, information technology, management information systems or equivalent
- Required - Structured project management experience in deploying security initiatives
- Required - Broad experience in computer and network systems, including IT security
- Required - Ability to handle ambiguity and make decisions and recommendations with limited data
- Required - Solid analytical/problem-solving skills with capability to identify solutions to unusual and complex problems
- Required - Excellent communications skills, including written, oral, and presentation
- Required - Experience leading security services and programs in the information technology sector.
- Required - At least five years' experience of increasing responsibility leading cybersecurity including IT governance, risk, and compliance services and programs culminating in a senior leadership role.
- Desired - Certifications and continuing professional learning demonstrating subject matter expertise in information security, risk, and/or privacy (e.g., CISSP, CRISC, CISA, CISM, CSX, etc.).
- Desired - Experience working with senior government or enterprise leadership regarding information security strategy, information security incident response, and information security governance.

Key Experts (3)

(a) Security Analyst
(b) Security Engineer
(c) Security Consultant

Overall qualifications and experience for the Key Experts

- Bachelor's degree in information and communication technologies or an equivalent combination of academic qualifications and work experience;
- Experienced ICT specialists, with relevant international transactional and project experience (minimum 10 years) in the business and ICT sector, preferably with experience in developing countries;
- Demonstrated experience with practical application of leading digital technologies, in particular related to cloud, data management; (applies for experts (b) and (c)

- Knowledge and experience of ICT sector security issues in the South Pacific region and/or other small island economies is highly desirable (applies to all experts)
- Certified in one or more internationally accepted security qualifications, including CISA, CISM, CISSP, CompTIA Security +, CSX, ISO 27001, NIST SP 800-53v5, or equivalent national or regional (ENISA) security qualification Expert (b)
- Certified or trained in one or more of the following security audit, risk assessment, and governance certifications/standards: CGEIT, CRISC, Open FAIR, ISO 31000, ISO 27005, NIST SP 800-60; (applies to all the experts)
- Network and IT Security administration experience (5 years); (applies to all).

The attention of interested Consultants is drawn to Section III, paragraphs, 3.14, 3.16, and 3.17 of the World Bank's "Procurement Regulations for IPF Borrowers" July 2016, Revised November 2017 and August 2018("Procurement Regulations"), setting forth the World Bank's policy on conflict of interest.

Consultants may associate with other firms to enhance their qualifications, but should indicate clearly whether the association is in the form of a joint venture and/or a sub-consultancy. In the case of a joint venture, all the partners in the joint venture shall be jointly and severally liable for the entire contract, if selected.

A Consultant will be selected in accordance with the Consultant's Qualification Based Selection (CQS) method set out in the Paragraphs 7.11 to 7.12 of the Procurement Regulations.

Further information can be obtained at the address below during office hours 09:00 to 16:30 hours.

Expressions of interest must be delivered in a written form to the address below (in person, or by mail, or by fax, or by e-mail) no later than ***4:30pm of Friday, 8th November 2019***

Attn: Chief Executive Officer
Ministry of Finance
Nuku'alofa Tonga Islands
Tel: +676 23-066
E-mail: ***bfaotusia@finance.gov.to*** *and copy to DCEO of Corporate Services at* ***qfukofuka@finance.gov.to***

ANNEX 1: Terms of Reference

Tonga Digital Government Support Project

Terms of Reference (TORs) for the Cybersecurity Consultancy Services (Consulting Firm) for developing and supporting information systems

A. BACKGROUND INFORMATION ON THE PROJECT

The Government of Tonga is in the process of implementing an eGovernment (Digital Government) Support Project supported by the World Bank with multiple components for developing supporting ICT infrastructure, information systems, citizen eServices, and other frameworks and architectures needed to meet goals and objectives within the Tonga Digital Government Strategic Framework (DGSF).

The Digital Government Support Project components are as follows:

Component 1. Enabling Environment and Continuous Improvements

1.1 Development of a Digital (e-Government) Government Strategic Framework (DGSF*).** The Tonga DGSF sets directions for the Government's use of Information and Communication Technologies (ICT) or digital technologies, with the ***ultimate intent of improving Government business process and workflow efficiencies, improving the quality of life for citizens and residents, ***while reducing the complexity for business transacting with Government.*** The Government has already undertaken ministry and agency consultations. The final DGSF will incorporate inputs from government stakeholders to ensure alignment with the Tonga Strategic Development Framework (TSDF) and agency specific strategic plans. As noted above, the DGSF is based on a, "whole of Government" approach, also providing the basis for the required governance, services delivery and implementation arrangements.

1.2 Legal and regulatory framework for Digital Government including Civil Registration and national ID systems. This subcomponent will finance advisory services for modernizing the legal and regulatory frameworks institutional and governance arrangements, data security, data protection, authentication protocols and processes, privacy, transparency, non-discrimination and support for digital transactions. This subcomponent will also finance advisory services to modernize policies, laws and regulations related to Tonga's CR and national ID systems, including to facilitate the other activities under this activity, to put in place data protection safeguards to strengthen privacy and prevent misuse of data, and to prepare Tonga's identity ecosystem to support digital government and the digital economy.

1.3 Expansion of the Government's Cyber Security Program. This subcomponent will finance consultancies and capacity building activities for the development of operational and administrative standards, assurance, monitoring, audit, and Cyber-Security Emergency Response (CERT) capabilities. The Cyber Security Program will also include comprehensive security training and awareness programs for all government users, government IT and security professionals, management, citizens, and the private sector.

Component 2. Government Enterprise Architecture

2.1 Informed and timely decision making. This subcomponent is to design and implement digital governance and decision-making processes to ensure timely and quality data and

information accessible for informed decision making and change management. This component focuses on mapping of the existing decision-making processes and workflows to determine strengths, gaps and weaknesses and to build and streamline for a more efficient systems with a view for continuous improvements.

2.2 National Enterprise Architecture. This component follows component 2.1 and will also finance the development of a Tonga Enterprise Architecture Framework (TEAF). The TEAF will guide Ministries and Agencies through the business objectives, information and data requirements, need for process and workflow mapping, and technology changes necessary to execute their information systems (consultancy, software development/purchase) strategies.

Components 3. Process Automation: Civil Registration and National ID Systems

3.1 ***Implementation of selected e-Services.*** This subcomponent will finance the development of selected

digital services, for example business registration and digital procurement based on a readiness assessment digital services, for example business registration and digital procurement based on a readiness assessment (institutional as well as technical). It will also support advisory services to implement modifications of associated business processes within the ministries and agencies.

Mobile solutions will be developed, on needs basis, to enable reach to users that do not have access to computers. This will include implementation of workflow automation, allowing better citizen and business access to Government e-services, with cross-agency integration when appropriate or feasible. To effectively implement workflow automation, inter-agency data sharing, and automation of individual digital services requires use of process mapping and business process modelling notation. The Government has already undertaken consultations on this with government agencies to identify potential priority services.

3.2 Upgrade of CR System. This subcomponent will finance technical assistance to upgrade the current CR system, including to: (a) assign unique national ID numbers to Tongan citizens and residents of Tonga through birth registrations, based on the linkages established under subcomponent 3.3; (b) link birth, death and marriage records on the same individual; (b) receive automated birth and death notifications from the health sector; (b) securely push notifications of registered births and deaths to approved third parties (e.g. to notify the national ID system of deaths); (d) enable approved third parties to securely validate information (e.g. the Social Registry validating information on beneficiaries); and (e) deduplicate CR records in the future, such as based on the information of the parents (e.g. their national ID numbers).

3.3 Upgrade of ID System. This subcomponent will finance the upgrade of the current national ID system. These include: (a) developing a software module or interface for approved third parties in the public and private sectors to digitally authenticate the identity of their customers based on information in the national ID system register, which may include biometric, biographic and/or One Time Password (OTP) yes/no verification; and, if applicable, (b) expanding coverage of the national ID system, including to citizens and residents of Tonga younger than 14 (through the issuance of a unique national ID number and not necessarily a card), possibly leveraging, where appropriate, the Social Registry enrollment exercise or the ORG's planned birth registration catch up campaign.

3.4 Development of CR-ID linkage. This subcomponent will finance the functional and technical integration between the CR and national ID systems, including building a software solution that facilitates automated exchange of data, such as to assign unique numbers from the national ID system at the time of birth registration and for the national ID system to receive information on registered deaths and to validate information at the time of enrollment.

Component 4 Digital Government Infrastructure

4.1 Design and implementation of a National Government Portal. This subcomponent will finance a single window to facilitate citizen and business access to public information, interactions and transactions with Government ministries and agencies. The Single Window will require a standard ("look and feel") Government agency landing page template to show continuity and consistency in the implementation of information services in each agency.

4.2 Design and implement the Tonga Government Cloud (G-Cloud). This subcomponent will finance the design and implementation of the G-Cloud, including data centers consolidation and information systems transition to the G-Cloud. The use of cloud services will entail partnership with the private sector which has the requisite technical and management expertise.

4.3 Design of Secure Government Network and Data Centers, including Disaster Recovery and Continuity of Operations Plan. This subcomponent will finance advisory services for designing the Digital Government Infrastructure and Platform to support information systems and applications for Ministry and Agency users. Proprietary and open source options will be considered. The component will consider and evaluate alternative data center or cloud computing ownership models taking into consideration climate change impacts, disaster risks security, resource management, operational and capital cost of operations, continuity of operations, and total cost of ownership.

Component 5 Project Management

5.1 Project management and technical support for the project. This component will finance technical Project management support for MEIDECC and MOFNP. The Project manager will assist MEIDECC and MOFNP with project management and coordination, communications, monitoring, and evaluation and reporting. Other aspects of Project administration (procurement, financial management, audit) will be handled by the Ministry of Finance and National Planning (MFNP) Central Services Unit. In addition, this component includes provision for full project documentation, logistics, consumables, office equipment, and incremental operating costs.

B. SCOPE OF WORK AND METHODOLOGY APPROACH

The Government needs to develop a Cybersecurity team to develop a comprehensive Cybersecurity program required within the Digital Government Component 1.3., ***Expansion of the Government's Cyber Security Program***.

This subcomponent will finance consultancies and capacity building activities for the development of operational and administrative standards, assurance, and monitoring, audit, and Cyber-Security Emergency Response (CERT) capabilities. The Cyber Security Program will also include comprehensive security training and awareness programs for all government users, government IT and security professionals, management, citizens, and the private sector.

The Cybersecurity Team will be led by the Cybersecurity Program Manager. The cybersecurity program manager in close collaboration with CERT Tonga and other relevant stakeholders will develop a Tonga National Cybersecurity Program, and implement the Cyber Security Program across all government Ministries, Departments, and Agencies (MDAs), in addition to making the Tonga Cybersecurity Program guidance available to private industry and the general public.

The Cybersecurity Program Manager will work with security, information systems, and MDA business leadership leadership/stakeholders to identify and plan physical and cybersecurity policies, standards, and procedures to assure compliance with Component 1.3. Additional responsibilities include, but are not limited to, assisting MDAs with Cybersecurity plans, audits, IT Cybersecurity project cost estimates, and general organizational security awareness training.

The Cybersecurity Consulting Team will include the following additional experts with the following responsibilities

- Security Analyst: Analyzes and assesses vulnerabilities in Information Systems architecture and operational infrastructure (e.g., software, hardware, networks). The Security Analyst investigates available Cybersecurity tools and mitigations needed to identify and resolve identified security vulnerabilities, and recommends solutions and continuing Cybersecurity design and operational best practices. The Cybersecurity Analyst will assess damage or loss to the data/infrastructure as a result of security incidents, and provide detailed reports to the Cybersecurity Program Manager and Minister of MEIDECC for communication and distribution to relevant government leadership.
- Security Engineer: Performs security monitoring, security and data/logs analysis, and forensic analysis, to detect security incidents, and manages incident response. Investigates and utilizes new technologies and processes to enhance security capabilities and implement improvements. Designs a security system or major components of a security system, and may head a security design team in defining new security standards / policies needed to implement new security systems and guidance.
- Security Consultant/Specialist: provides Cybersecurity implementation support, including consultancy services for MDAs and MEIDECC ICT operations. Develops Cybersecurity communication plan and communication awareness training for all Tonga MDAs, private industry, and general public.

C. ACTIVITIES TO BE UNDERTAKEN BY THE CONSULTANT (Consulting Firm)

Cybersecurity Consultants' Main Duties and Responsibilities

- Lead the Tonga Cybersecurity Program, including development and management of Cybersecurity services, and products
- Develop Tonga Cybersecurity standards, adopting international government and generic (ISO) standards applicable to the Tonga government, business, and public environment.
- Manage development and delivery of ongoing program components including
    - Identifying and securing resources for program development
    - Managing the phased development and implementation of the program
    - Coordinate with MDA stakeholders to ensure broad understanding of MDA requirements, vulnerabilities, mitigations, and standards compliance
    - Cybersecurity program innovations and global currency
    - Cybersecurity program communications and awareness activities
    - Recurring Cybersecurity self-assessment and formal audit programs
- Provide technical support to the Tonga Cybersecurity Emergency Response Team (CERT) enhancement program.
- Develop initial and recurring Cybersecurity training and awareness program for all government employees
- Develop minimum Cybersecurity skills and certification requirements for Tonga network, software development, and information systems management staff.
- Establish and manage Cybersecurity Program Office
- Transfer knowledge and build capacity of permanent Government staff

QUALIFICATIONS AND PROFESSIONAL EXPERIENCE REQUIREMENTS OF THE CONSULTING FIRM

The following minimum qualifications and experience are required and will be used to evaluate the potential consultants (consulting firms). The consulting firm should be qualified and experienced for carrying out this assignment. The firm should demonstrate at least 10 years of experience in similar services and at least 3 contracts of similar assignments successfully performed for the last five (5) years. The consultant will propose a team of Experts that will include the following specializations:

Team Leader (1)

Qualifications and Experience

- Required - Degree in electrical engineering, systems engineering, computer science, computer engineering, information technology, management information systems or equivalent
- Required - Structured project management experience in deploying security initiatives
- Required - Broad experience in computer and network systems, including IT security
- Required - Ability to handle ambiguity and make decisions and recommendations with limited data
- Required - Solid analytical/problem-solving skills with capability to identify solutions to unusual and complex problems
- Required - Excellent communications skills, including written, oral, and presentation

- Required - Experience leading security services and programs in the information technology sector.
- Required - At least five years' experience of increasing responsibility leading cybersecurity including IT governance, risk, and compliance services and programs culminating in a senior leadership role.
- Desired - Certifications and continuing professional learning demonstrating subject matter expertise in information security, risk, and/or privacy (e.g., CISSP, CRISC, CISA, CISM, CSX, etc.).
- Desired - Experience working with senior government or enterprise leadership regarding information security strategy, information security incident response, and information security governance.

Key Experts (3)

(d) Security Analyst
(e) Security Engineer
(f) Security Consultant

Overall qualifications and experience for the Key Experts

- Bachelor's degree in information and communication technologies or an equivalent combination of academic qualifications and work experience;
- Experienced ICT specialists, with relevant international transactional and project experience (minimum 10 years) in the business and ICT sector, preferably with experience in developing countries;
- Demonstrated experience with practical application of leading digital technologies, in particular related to cloud, data management; (applies for experts (b) and (c)
- Knowledge and experience of ICT sector security issues in the South Pacific region and/or other small island economies is highly desirable (applies to all experts)
- Certified in one or more internationally accepted security qualifications, including CISA, CISM, CISSP, CompTIA Security +, CSX, ISO 27001, NIST SP 800-53v5, or equivalent national or regional (ENISA) security qualification Expert (b)
- Certified or trained in one or more of the following security audit, risk assessment, and governance certifications/standards: CGEIT, CRISC, Open FAIR, ISO 31000, ISO 27005, NIST SP 800-60; (applies to all the experts)
- Network and IT Security administration experience (5 years); (applies to all).

D. EXPECTED DELIVERABLES/OUTPUTS WITH TIMELINES

The intent for all tasks and requirements is to develop standards, frameworks, processes, and skills needed for Tonga Government agencies – and the general public – to improve the overall security profile and capabilities of Information and Technology systems across government. It is expected at the end of the contract; security operations will be the responsibility of Tonga Government MDAs. Based on duties and responsibilities, the expected key deliverables/outputs are as follows:

Functional Area	Activities with Deliverables

Cybersecurity Governance	1. Provide an inception report including a detailed work plan
	2. Develop National Cybersecurity Framework and Submitted for Approval
	3. Conduct a Cybersecurity audit and risk assessment of all Tonga Government agencies starting with the Government Data Center and SGN using guidelines established in an international standard such as ISO 27001, ISO 27005, ISO 31000, NIST SP 800-60; and submission of audit and assessment report with recommendations
	4. Record all audit findings in a combined security risk register
	5. Prepare risk mitigation plan for all security vulnerabilities identified in security audit and assessment
	6. Develop and implement recurring Cybersecurity Awareness training programme
	7. Establish an Information Security Management System and provide an implementation manual
Cybersecurity Emergency Response Team / CERT	8. In close collaboration with CERT Tonga and other relevant stakeholders, address the gaps within the established CERT Program, including staffing plan
	9. In close collaboration with CERT Tonga and other relevant stakeholders, develop recurring national security awareness training plan for both government and general public
	10. Enhance the CERT operations processes and checklists through review of current CERT operations and practices.
Security Operations	11. Select required security tools to manage the daily security operations and provide a recommendation report.
	12. Contract 3rd party for security assessment services
	13. Develop and Implement standards and processes for ensuring preventive, detective and corrective measures (especially up-to-date security patches and virus control) across the Government to protect information systems and

	technology from malicious threats (e.g., APTs, ransomware, malware, viruses, worms, spyware, spam); provide implementation guidance.
	14. Implement security measures and related management procedures to protect information over all methods of connectivity including SGN and individually procured Internet connections; provide implementation strategy and guidance/manual.
	15. Design an operational security management, identity, and authentication/access system and processes
	16. Define and implement security procedures (including emergency procedures) to grant, limit and revoke individual access to data centers, server rooms, and communications hubs, according to business need and provide an enabling policy including supporting guidelines and manual.
	17. Implement other security processes required or relevant from international or Tonga security standards
	18. Conduct security operations training g (minimum 3 sessions) for all security operations staff on the requirements for implementing and maintaining either select international security standards or Tonga Security Standard (if available)
	19. Provide guideline to assist Government to recruit and train staff in areas including security audit, monitoring and management.
	20. Establish security and risk review process guideline for all new applications, services, and data systems implementations across all MDAs (including those systems provided by NGOs or other special interest groups)

E. DURATION OF THE ASSIGNMENT AND ESTIMATED EXPERT-TIME INPUT

The assignment is expected to commence in November 2019. The overall assignment is expected to require about 250 working days spread over 18 months. Remuneration will be based on a lump sum assignment, linked to a final agreed list of deliverables/outputs. A minimum of four visits for the firm and its key personnel to Tonga will be required, with a minimum duration of two weeks, preferably more.

F. CONFIDENTIALITY

The Consultant shall keep all information provided by the client in confidence. The Consultant shall only use the confidential information in connection with the performance of the project and for no other purposes. This provision will be incorporated into the consultant's contract.

G. REPORTING REQUIREMENTS

The consultant shall report directly to the CEOs of the Ministry of Finance and MEIDECC through the TDGSP Project Manager. This assignment will be coordinated by the Project Manager and the consultants/firm will work closely with the implementing agencies for technical advice and information.

H. ADMINISTRATIVE ARRANGEMENTS

The consultant will be engaged by MOF. Payment will be made by MOF after its confirmation that the required milestones and works are complete. Travel, accommodation and expenses arrangements will be negotiated with the Ministry, but the standards and procedures of the World Bank will be used as a benchmark. Travel, accommodation and expenses will only be paid for working stays in Tonga.

This procurement process will be conducted in accordance with the World Bank Procurement Regulations for IPF Borrowers, July 2016 ("Borrower Regulations") https://policies.worldbank.org/sites/ppf3/PPFDocuments/Forms/DispPage.aspx?docid=4005

A Consultant will be selected in accordance with the method set out in the Borrower Regulations for Selection of Consultants through the Consultants' Qualifications Selection (CQS) procedures.

Further information regarding this consultancy services can be obtained by contacting:

Mrs. Balwyn Faótusia

CEO, Ministry for Finance

bfaotusia@finance.gov.to

St George Palace

Nukuálofa