Government of JERSEY

EXPRESSION OF INTEREST (EOI)
INFORMATION SECURITY GOVERNANCE SERVICES
EOI REFERENCE: CS20/01/005

NOVEMBER 2019

Expression of Interest (EOI)

This is an Expression of Interest (EOI) notice. The Government of Jersey (GoJ) wishes to contract with a supplier that will provide a **Information Security Governance Service** to be delivered into the organisation through the Government's **Cyber Security Programme.** The GoJ is managing this procurement process in accordance with the Jersey Financial Directions.

If this opportunity is of interest, please register your interest on the Government's procurement portal www.channelislandtenders.com

The purpose of the Expression of Interest is to provide potential service providers with an overview of the Governments requirement and the proposed timeline for procurement.

About the Government of Jersey

The Government of Jersey (GoJ) is the government (www.gov.je) of the Island of Jersey and is responsible for the management of the Island's finances and operation of its public services. Jersey does not sit within the European Union but as a Public Sector body it applies the principle of transparent procurement practices in accordance within the boundaries Jersey laws and financial regulations.

Jersey is self-governing with independent fiscal and legal systems and courts of law. The States Assembly is made up of 49 elected members. Jersey is a British Crown Dependency and is defended and internationally represented by the UK government. The population of Jersey is estimated at 104,000 with population density being approximately double that of England.

Jersey is in a unique position of fulfilling the majority of roles of both a central and a local government but scaled to a small jurisdiction. This presents challenges in delivering economies of scale, but also huge opportunity to more easily join up processes across the entire system of government administration.

The Government have set out a long-term vision and ambition for modernising and improving Jersey's public services which can be further understood by reading the following documents;

Proposed Government Plan 2020-2023,

The proposed Government Plan sets out the income and spending proposals in one comprehensive, costed plan. Ministers have published their first-ever Government Plan for Jersey. The plan brings to life the five strategic priorities that the States Assembly unanimously approved for this Government's term of office.

Common Strategic Policy,

The Common Strategic Policy sets out ministers' high-level ambitions for Jersey and contains five strategic priorities where ministers will focus their efforts.

In addition, Future Jersey and the Island Plan provide insight into the longer term strategic plans and sets out Islanders' ambitions for Jersey's future over the next 20 years.

About the Government Transformation Programme (OneGov)

The Government of Jersey ("the Government") has recently undertaken steps to transform its organisational structure. To help achieve its goals, the Government will reorganise public services to become one government and integrate the delivery of services to islanders, providing coherence and clarity about our structure, accountabilities and performance.

The delivery of this transformation will be realised through the implementation of a range of initiatives and will be critically dependent on technology. However, the Government has to deal with a substantial "technology debt", a historical lack of investment in digital and technology capability and a shortfall in capacity to handle current demand. Significant upfront investment is required to address this situation and achieve the outstanding, modern public services that our islanders and employees deserve.

Further information on this area can be found in the Modernising Government section of the Government Plan (Section 2, Part 6)

About the Cybersecurity Programme

As the Government of Jersey embarks on a period of extensive change and modernisation, Cybersecurity has become a critical enabler for a large number of programmes and business-as-usual activities. The Government of Jersey IT department (Modernisation and Digital Department) is currently transforming to better serve the Government and the citizens of Jersey; as part of this Cybersecurity capabilities shall be improved in quality and in scale. A comprehensive maturity assessment of Cybersecurity was conducted in 2019 which identified areas for development and improvement within the Government. The results of the maturity assessment have been used to design the Cybersecurity Programme which will be structured into two 12-month tranches with Tranche 1 being split into five distinct projects:

- Design and provision of a Managed Security Service for the Government of Jersey
- Information Security Governance Improvement
- People Security Improvement
- Asset Management Improvement
- Identity and Access Management Improvement

The Government of Jersey published its Cyber Security Strategy in 2017 which shows the role of the Government in the journey to make Jersey a safe and secure place to live and work.

The Government is now seeking professional support and subject matter expertise from a qualified and experienced supplier to deliver Information Security Governance across the Government of Jersey, which will provide over-arching control and decision-making support throughout the organisation.

It is anticipated that this project will commence in March 2020 with basic monitoring and reporting capabilities being in place by July 2020. The development of this capability will be delivered over the first two years of the Programme.

Summary Overview of Requirements

The provision of the Information Security Governance Service will provide a greater foundation for effectively identifying and managing risks facing the Government of Jersey. It will provide over-arching control and decision-making support throughout the organisation. The Project will deliver the services shown in the diagram below.

1. Cyber Security Governance Improvement – Management and Business Change					
2. Governance Improvement				3. BaU Process Support	
2.1 Risk Management Process	2.2 Information Security Metrics and Reporting	2.3 Information Security Governance Documents Improvement	2.4 Operational Technology Governance Improvement	3.1 Programme Security Support	3.2 3rd Party Supplier Risk Management Support

The requirements for the Governance Project are divided into the following sections:

1. **Cyber Security Governance Improvement Project Governance and Business Change** – The project is part of the Cyber Security Programme and will lead the Project's Business Change capability to ensure that all delivered outputs, outcomes and benefits are embedded into the Government of Jersey. This will involve:

    1) Managing the Governance Project and aligning all Project governance and reporting to the Cyber Security Programme's established processes.
    2) Leading Business Change activities for the Governance Project to ensure that all delivered outputs, outcomes and benefits are realised and managed. This will align with the Cyber Security Programme's established Business Change processes.

2. **Governance Improvement** – These work streams will improve the ability of the Government of Jersey to understand and manage its Information Security capabilities and posture. It involves the following work streams:

    1) **Developing a Cyber Security Risk Management process:** The selected supplier will be required to develop a Cyber Security Risk Management process that is sustainable after the closure of the Cyber Security Programme. It should enable the identification, reporting and management of cyber security risks from across the whole Government and it should align with Government Enterprise Risk Management processes (which are currently under development). This will involve:
        - Developing a Cyber Risk Identification and Reporting process that allows gathering and reporting of risks from across the whole organisation to the Information Security Team
        - Developing a Cyber Security Risk management process which aligns management actions to risks and gives clear risk metrics to the Information Security Team and the Risk Management Team.
        - Developing and implementing any risk management products (e.g. registers, databases etc.)
        - Implementing the developed Cyber Security Risk Management process into the Information Security Team with required links across Government established to enable the capability to function fully.

2) **Developing Information Security metrics and reporting:** The selected supplier will be responsible for developing an Information Security metrics and reporting capability that will demonstrate the state of Cyber Security capabilities and the Information Security Risk the organisations. This will involve**:**
    - Working with all levels of the Government to design a set of Key Performance Indicators (KPIs) and metrics which will be meaningful to the relevant people and teams.
    - Developing an Information Security metrics collection, processing and reporting process
    - Creating a reporting templates that will allow various levels of the organisation to take actions based on the state of Information Security capabilities and risks.

3) **Governance documentation improvement:** The Government of Jersey is looking to align to ISO 27001 Information Security Management System. The selected supplier will be required to support the Government in developing existing and writing new Information Security governance documentation (i.e. Policies, Standards, Processes and Guidelines). These will be the foundation of Information Security Governance across the Government. This will include:
    - Creating an Information Security Policy Framework for the Government of Jersey detailing all required Information Security governance documentation
    - Identifying all required polices, standards etc. required for Information Security governance in the Government of Jersey
    - Reviewing and updating the current policies, standards etc. as appropriate
    - Writing new policies, standards etc. to govern key aspects of Information Security in the Government of Jersey as appropriate
    - Communicating all policy changes to appropriate audiences
    - Delivering all policies into an appropriate policy management capability
    - Designing and embedding a policy review process
    - Reviewing and updating all policies, standards etc. dealing with internal and external information sharing within the Government of Jersey and between the Government and other quasi-government organisations

4) **Operational Technology (OT) Security Governance Improvement:** The Government of Jersey has a number of services which use Operational Technologies (OT)including the Energy from Waste Plant and Telemetry systems. These are not currently fully integrated into the Government's Information Security Management processes. The supplier will be required to review and update all existing OT security management policies, standards etc. and processes to bring their management and reporting in line with the Information Security Team's requirements. This will include:
    - Reviewing and updating the current Information Security Management processes and governance of OT solutions deployed across the Government

- Integrating the Government of Jersey Cyber Incident Response Plan with the OT Security Response Plan
- Setting up meaningful reporting of Information Security capabilities, the status of them and the Information Security Risks held by the OT estate

3. **Business as Usual (BaU) Support –** These work packages aim to accelerate the implementation of key Information Security services to Government of Jersey. This will include:

    1) **Providing Security Architecture support to Technology and Security programmes/projects:** The selected supplier will be responsible for assessing all current Technology and Security related programmes and projects running in the Government of Jersey to identify high risk programmes/projects and provide security support to them. The Government of Jersey will employ permanent security architects at some point (TBD) during Tranche 1 of the Cyber Security Programme. Therefore, the supplier will hand over to these permanent employees once they arrive as employees of the Government. The supplier will:
        - Design and conduct an assessment of all Technology and Security projects and programmes being delivered across the Government.
        - Provide security architecture support to the 10 highest-risk Technology and Security related programmes and projects
        - Hand over the Programme/Project Risk Assessment tools and processes, as well as the security architecture support for the 10 highest risk Technology and Security related projects to the incoming permanent Security Architects.

    2) **Providing 3rd Party Supplier Risk Management support to Technology and Security service suppliers:** The selected supplier will provide support to the 3rd Party Supplier Risk Management process to enhance the way the Government of Jersey selects, assesses and oversees the 3rd party security. The Government of Jersey will employ permanent 3rd Party Supplier Risk Management team members at some point (TBD) during Tranche 1 of the Cyber Security Programme. Therefore, the supplier will hand over to these permanent employees once they arrive as employees of the Government. The supplier will:

        - Review and, where appropriate, improving Government of Jersey standard contractual terms and conditions to ensure that they are fit for purpose from an Information and Cyber Security perspective.
        - Identify and assess all 3rd party suppliers' contracts for Technology and Security services that the Government of Jersey currently holds
        - Review and update all IT and Security contractual agreements as required
        - Develop a 3rd Party Supplier security audit assessment that will test, verify and evaluate the effectiveness of a 3rd Party's risk management controls
        - Conduct an audit on the organisations which hold the 5 highest risk contractual arrangements with the Government of Jersey
        - Develop reporting and risk management processes for 3rd Party Risks.

- Hand over all developed products, assessments and work to the incoming permanent 3rd Party Supplier Risk Management team members.

Consortia and Sub-Contracting

The Government is open to receiving expressions from either single organisations or a consortium of organisations with proven experience of delivering similar capabilities.

Procurement Route, Contract Type and Conditions

Standard GOJ contract terms and conditions for services shall apply to this tender.

Programme- Anticipated Dates and Locations

The proposed contract period is anticipated to be from March 2020 to March 2021. These are indicative dates and the Government of Jersey maintains the right to change these dates as required.

Activity	Date
Expression of Interest Issue Date	24 January 2020
Expression of Interest Close Time & Date	14 February 2020
Pre-Qualification Questionnaire and Invitation to Tender Issue Date	29 January 2020
Pre-Qualification Questionnaire and Invitation to Tender Close Date	19 February 2020
Supplier presentations / interviews	3 March 2020
Evaluation process complete	13 March 2020
Preferred supplier notified	W/c 16 March 2020
Contracts signed	W/c 23 March 2020
Contract start date	W/c 23 March 2020

The principal location for the work will be 18-22 Broad Street, St Helier, Jersey.

It is anticipated that a significant amount of engagement with Government of Jersey stakeholders will be required to deliver the project. This will require co-locating with the programme team and having on-site presence for a substantial part of the initial phase of engagement in Jersey.

EOI Submission Process and Deadline

Please register your interest using the Government's Procurement Portal at www.channelislandtenders.com.

Please Note: Suppliers expressing an interest are advised that nothing herein or in any other communication made between the GOJ and any other party, or any part thereof, shall be taken as constituting a contract, agreement or representation between the GOJ and any other party (save for a formal award of contract made in writing) nor shall they be taken as constituting a contract, agreement or representation that a contract shall be offered in accordance herewith or not at all.

Should GoJ decide to publish an ITT, suppliers expressing an interest shall receive notification through the Government's Procurement Portal. Potential suppliers who do not respond to the EoI may still respond to the ITT.