Government of JERSEY

EXPRESSION OF INTEREST (EOI)
FOR DESIGN AND PROVISION OF MANAGED IT SECURITY SERVICE (MSS)
EOI REFERENCE: CP19/11/787

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 **Managed IT Security Services** to be delivered into the organisation through the Government's upcoming **Cyber Security Programme.** The GoJ is managing this procurement process in accordance with the Jersey Financial Directions. This services contract is being procured using a two -stage "restricted process" procedure.

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

- 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 Information Security Team are part of Modernisation and Digital which is also about to embark on a large-scale change programme. This will fundamentally change the operating model of the department and will introduce new capability groups – including growth of the security function and the establishment of an architecture capability. The Government of Jersey is also transitioning its core IT capabilities into the Microsoft 365 cloud environment. Both programmes will need to be considered throughout delivery and management of the managed security service.

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 Managed Security Services Provider to design, implement and run a managed security solution for the Government’s technology enterprise.

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 and tuning of this capability will be delivered over the first two years of the Programme.

Summary Overview of Requirements

The provision of a **Managed IT Security Service** for the Government of Jersey will deliver the foundation for a comprehensive, integrated technology suite to detect, monitor and protect against information security threats and vulnerabilities. The selected provider will assist in the design, build and operation of strategic security controls that form the basis for future evolution of detection and prevention capabilities that defend the GoJ and dependant entities from cyber-attack.

The requirements for Managed Security Service Provision is divided into the following areas:

1. Design and Implementation of a Comprehensive Defensive Technology Suite for the GoJ

   The successful service provider will be required to work with the Modernisation & Digital team to design a suitable architecture and provide the supporting technology to protect and monitor endpoints, networks, and cloud environments, detect unusual or prohibited behaviours to proactively identify potential compromises and prevent the disruption of services. The implementation of such tools will enhance the resilience of the GoJ to cyber-attacks and protect its most critical services and assets.

   a. Design and implement technical security controls that complement existing investment in defensive capabilities that protect Government systems and data assets from deliberate or accidental compromise and disruption of services provided to Government employees and the citizens of Jersey.
   b. Proposed Controls should include but not be limited to Intrusion Detection / Prevention, Data Loss Prevention, Cloud Security Gateways, Web Gateways and Security Monitoring / Analytics.
   c. Host-based controls and securing cloud-based services including O365 should be considered as part of a holistic solution where these provide demonstrable benefit to the detection and remediation of prioritised threats to GoJ assets and services.

2. Design and Implement a Comprehensive Vulnerability Management Capability

   The selected MSSP will be required to work with the Modernisation & Digital team to develop and enhance the way the Government of Jersey identifies, assesses, prioritises, manages and reports vulnerabilities. The GoJ will require support and guidance to remediate high risk findings and patch outdated systems in defined timelines with minimal impact to its operations. A clearly defined methodology will help promote good security hygiene throughout the organisation.

   a. Review and improve the current approach to the detection and management of vulnerabilities that impact the secure operation of GoJ platforms and services.
   b. A capability will need to be proposed that considers the current and future requirements for vulnerability identification and the management and oversight of remedial activities including patching and implementation support/advice for approved workarounds that mitigate the impact of a potential compromise.
   c. The GoJ network and dependent entities have evolved over time with a diverse range of systems (including IT and OT systems) and varying levels of maturity. The posture of the environment within scope will need to be considered as part of the proposed Vulnerability Management capability.

3. Managed Security Service Provision

   The Government of Jersey is seeking a strategic partner in the provision of Managed Security Services to handle the day to day device management and monitoring of security capabilities, provide regular reporting in relation to the organisation's security posture and effectively assess, investigate and respond to security incidents..

The selected provider will be required to conduct an assessment of currently deployed cybersecurity technologies and provide an informed view on the best balance of re-using existing capability, introduction of new capabilities from with their existing product portfolio and applied innovation to deliver the desired service and best value to the GoJ, The contract will have the potential to be re-evaluated to increase the scope of service and optimise capabilities within the next year to drive automation and service improvements.

a. The selected provider will need to consider immediate requirements for the management and integration of proposed capabilities that address identified areas requiring improvement as well as providing future tuning and optimisation of services provided to GoJ within later tranches of the Cyber Security Programme.
b. The MSSP will be expected to propose and provide details of the tools that will be used to manage the proposed security capabilities and define the necessary requirements for integration with existing GoJ security capabilities and business systems that support issue resolution and incident management.
c. Details of current in scope systems, network architectures and existing security controls will be provided during the tender process, the selected MSSP will be expected to make recommendations for the novation and re-use of existing controls that, where appropriate, are complementary to the services being proposed.
d. A key aspect of the security services that GoJ is seeking to procure is the outsourcing of Security Monitoring and initial Incident Response. The MSSP will be required to propose an end-to-end SOC service and supporting capability. The MSSP will be expected to define the requirements for security event data acquisition and the development of detection logic that fulfils the GoJ requirements for initial monitoring capability and incident triage.
e. The MSSP will be required to work with the Modernisation & Digital Information Security Team and IT Operations Team to develop the concept of operation and incident management playbooks that define the role of the SOC. The MSSP will be expected to propose tested and exercised processes and supporting analytics so that the SOC is delivering value to GoJ from day one.
f. The MSSP will be required to define how they propose to acquire and leverage high fidelity Threat Intelligence within the provision of managed security services.
g. The MSSP should propose methods of automation and orchestration that will drive service improvement, optimisation and cost reduction in future tranches of the Cybersecurity Programme.
h. The MSSP will be expected to provide reporting of key metrics and risks relating to Government systems. These metrics and reports should be developed in consultation with the Government Information Security and Technology Teams.

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. Tenderers are required to comply with the key contractual terms and conditions in the contract with no suggested material amendments/mark-ups. The Government is open to any form of commercial arrangement for the design, implementation and management of the delivered service – this should be recommended by the suppliers.

Programme- Anticipated Dates and Locations

The proposed contract period is anticipated to be from March 2020 to March 2022.

Activity	Date
Expression of Interest Issue Date	Friday 21st November 2019
Expression of Interest Close Time & Date	Friday 20th December 2019
Pre-Qualification Questionnaire Issue Date	Monday 2nd December 2019
Pre-Qualification Questionnaire Close Date	Friday 20th December 2019
Invitation to Tender Issue Date (to top 3 suppliers)	w/c 13th January 2020
Tender close time & date	w/c 27th January 2020
Supplier presentations / interviews (if required)	w/c 10th February 2020
Evaluation process complete	w/c 17th February 2020
Preferred supplier notified	w/c 17th February 2020
Contracts signed	Friday 21st February 2020
Contract start date	Monday 24th February 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 to have 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.