**United Nations** **Nations Unies**

Procurement Division
New York

# REQUEST FOR EXPRESSION OF INTEREST (EOI)

**Title of the EOI:**
Provision of Infrastructure-as-a-Service (IaaS) for UNJSPF

**Date of this EOI:** 14 January 2020

**Closing Date for Receipt of EOI at PD:** 14 February 2020

**EOI Number:** EOIJK717111

**Address EOI response by fax or e-mail to the Attention of:** Joniolavi Kaerpijoki

**Fax Number:**

**E-mail Address:** joni.kaerpijoki@un.org

**UNSPSC Code:** 81112100, 81112000, 43212200, 81112003, 81161500, 81111900

## DESCRIPTION OF REQUIREMENTS

The Office of Investment Management ("OIM") of the United Nations Joint Staff Pension Fund ("UNJSPF") is seeking services of qualified Infrastructure-as-a-Service (IaaS) providers to support its investment operations. The main areas of service that OIM is looking for include the following:

- The Operations and Information Systems Section has incorporated cloud computing into its strategy with the aim of increasing agility and lowering costs on new IT related projects that require significant infrastructure resources. OIM's vision is that these infrastructure resources will be rapidly provisioned and released for OIM on an on-demand basis within the predefined thresholds as defined in the SLA and that the solutions developed on top of these services will be able to preserve an adequate level of data portability, cloud interoperability and security.
- Among the different cloud computing service and deployment models, OIM's interest focuses specifically on Self-Managed Public Cloud based Infrastructure as a Service (IaaS) offerings that will replace traditional data center infrastructure.

Overview of the Fund

1. The United Nations Joint Staff Pension Fund (UNJSPF) is a defined benefit fund, established by the General Assembly of the United Nations (UN) in 1948. The Fund is charged with providing retirement, death, disability and other benefits and related services to its participants, retirees and beneficiaries, currently comprising over 205,000 staff and retirees of the United Nations and 23 other international inter-governmental organizations admitted to membership in the Fund.
2. The United Nations Secretary-General is responsible for the investment of the assets of the UNJSPF.

The Secretary-General has delegated this responsibility to the Representative of the Secretary-General for the investment of the assets of the UNJSPF (RSG). The RSG is, in turn, assisted in this function by the Office of Investment Management (OIM) of the UNJSPF

3. OIM manages a multi-asset class, global investment portfolio worth $65.6 billion as of 1 September 2018, about 85% of which is actively managed in-house. OIM invests globally in over 100 countries and regions distributed in 26 currencies and in both publicly traded securities as well as private capital investments. Asset classes under management comprise global equities, global fixed income, foreign exchange, private equity, real estate, infrastructure, timber, and commodities. OIM's staff are currently all based in New York but come from over 30 countries. Please consult OIM's website at https://oim.unjspf.org/ for additional information and a breakdown of the UNJSPF's assets.

4. The Operations and Information Systems Section (ISS) provides IT Services to the Office of Investment Management (OIM). It is responsible for providing ICT Infrastructure to support the day-to-day operations of the ICT business applications that ensure the security of the Fund's investments and supporting the front-to-back investment operation processes.

5. The provision of ICT Services has been developed and expanded as OIM has expanded over the years. Information Technology is key component of overall service delivery of the OIM and its stakeholders. There are currently 11 IT Staff.

6. OIM currently uses on-premise ICT Infrastructure managed and supported by a third-party service provider in a multi-tenant environment in North America and Europe.

7. OIM's ISS operates 24 hours a day, 7 days a week first level Service Desk support and receives requests for support by phone, text, email and self-service using the ITSM tool. OIM/ISS will remain responsible for global administrator and change manager. OIM/ISS will remain responsible for configuration, roles and access management and licensing as well as maintenance, upgrades and release management along with user acceptance testing (UAT) and production support.

**SPECIFIC REQUIREMENTS / INFORMATION (IF ANY)**

Scope of Work:

A - Network Infrastructure Service and Support

LAN

A-1) Provide support with DNS, DHCP, NTP, SNMP, as well as basic requirements for caching, VLANs, and segmentation.

WAN

A-2) Provide network support for connectivity to UN Headquarters (UNHQ) over the UNHQ MPLS and UNJSPF Secretariat. Support and enable MPLS on all managed devices as requested by OIM

A-3) Support and enable Quality of Service (QoS) and bandwidth utilization reports on all devices as requested by OIM. Continuously monitor performance of network traffic, backbone links and network devices and take appropriate effective remedial action when alerts are activated.

Network Infrastructure

A-4) Internet Protocol Security Virtual Private Networks (IPSEC VPNs) between in house and Cloud hosted Machine instances. Traffic management mechanisms to implement both performance and availability-based load balancing, and controlled caching and geographic dispersion of static content to provide CDN services and seamless transition between primary and secondary.

A-5) Provide redundant NOCs for increased coverage and assurance.

A-6) Access to OIM network must be in compliance with the provided procurement and compliance policies for OIM ICT User Management.

Resource Pooling and Rapid Elasticity

A-7) Near real-time service provisioning and de-provisioning times.

Network Monitor

A-8) Provide a dashboard for the all network services including utilizations, availabilities, capacity, and bandwidth usages

A-9) Provide estimate for network downtime during the year. The availability of network must be maintained at 99.99 percent or better.
A-10) Perform root-cause analysis on network-related problems and implement effective solutions to mitigate their effect and prevent their recurrence.
A-11) Monitor all scheduled activities including data backup and detect and rectify any failure within agreed timeframes.
A-12) Provide regular and on-demand reports detailing network operations (performance/reliability).
A-13) Incorporate the ability to capture traffic and provide network interface statistics on-demand as requested by OIM to assist in troubleshooting and investigations.
A-14) Conduct audits of the OIM's ICT equipment, network, etc. as requested, and provide a report with suggestions regarding ongoing security needs of OIM.
A-15) Provide environmental requirements and report on any known or discovered temperature and/or power conditions that would impact or have the potential to impact performance.
A-16) Maintain up-to-date documentation and Configuration Management Database (CMDB) for all vendor-managed devices to include device identification, operating systems versions, patch levels, configuration settings, and change history. This documentation must be securely available online to OIM.

Response times and escalation procedures
A-17) Provide standardized communication templates to notify affected users of any scheduled or unscheduled service interruptions within a specific timeframe (within 4 hours), in accordance with a Communications Plan to be developed collaboratively with OIM.
A-18) Scheduled service interruptions shall follow the established change management processes and integrate with our IT service management solution.
A-19) The service provider must provide details related to response times and escalation procedures; must have a 24x7 support; must have self-service capabilities

Vendor's Client Portfolio
A-20) Provide access to Certified Engineers for design or change support. Upon request, provide OIM with certification verification information for its proposed staff (e.g. CCIE #, or proof of certification, etc.).
A-21) Provide ongoing evaluation and recommendation of new technologies in order to enhance and improve service and reduce costs of service.
A-22) OIM is Cisco standardized. Provide the benchmark of the hardware to be used for the Infrastructure implementation. Provide a detailed network diagram and the power requirements and identify those responsible for on-site maintenance.

Backup and Restore
A-23) The solution should use global deduplication algorithm at the source resulting in optimal LAN/WAN network bandwidth utilization as well as backup job time.

B – Platform Service and VM Service

B-1) Provision production, test and dev servers, storage appliances, virtualization platforms / hypervisors, Microsoft Active Directory and related components, application virtualization/presentation/delivery systems, database management systems and related components, middleware/integration platforms and related management systems & utilities.
B-2) Licensing and support of operating systems with relevant health, security, hygiene and 24/7 monitoring of performance, availability and capacity management. Provider should be able to manage existing OIM licenses, specific to clients. Provider must support and maintain WordPress based website and licenses, if any

Storage
B-3) Allocate standard and custom CPU and RAM, Cloud file system with container-based organization and object level access management with highly scalable and secure provisioning. Utilization of intelligent compression and eliminate redundant copies of data to reduce storage overhead and costs.

Mobile Office and Virtual Desktop Support

B-4) The network should be expanded based on international roaming, mobile office and virtual desktop support from home office or hot site locations as per OIM's requirements.
B-5) All software must be maintained and kept up-to-date. This includes the implementation of the most up-to-date and stable security patches, service packs etc. issued by manufacturers. Indicate the release schedule, downtime, and maintenance windows following standard industry practices with ample notification period.

APIs and Other Interfaces

B-6) REST / Query and SOAP APIs with support and complete documentation for each of the services and integration points as required by OIM.
B-7) Provider should manage their own Configuration Management Database (CMDB), Configuration Items (CIs), and be able to provide a feed into OIM's CMDB.
B-8) Provide the ability to feed logs into the OIM's ManageEngine.

C - Managed Security Services

Security Services

C-1) Provide support with management/administration of:
• Firewalls (Checkpoint, Cisco)
• Identity Service Engine
• Cisco Web Security Appliances
• Cisco Secure VPN
• Identity Management Service
C-2) Provide with security patches distribution tool to ensure that patch levels of all network devices are up-to-date in concurrence with OIM within the predefined maintenance windows.
C-3) Complete and provide to OIM a SOC2 Type II or equivalent attestation report on an annual basis, to be performed by an independent Certified Public Accountant or similar. The report shall include the Trust Services principles of Security and Availability. The report shall cover a 12-month period each year, without any gaps in coverage.
C-4) Perform quarterly security review and provide guidance in terms of technology innovation to provide a roadmap for the future. Shall provide meeting notes within five (5) business days of the review meeting. OIM will initiate and approve the agenda, location and participants.
C-5) Reconfiguration work undertaken by the provider must not compromise the security of the configurations
C-6) Conduct regular audits of the Authority's ICT equipment, network, etc. as requested, and provide a report with suggestions regarding ongoing security needs of OIM
C-7) Provide multi-factor authentication for all network access authentication, privileged security account access auditing, and risk-based and location based authentication.
C-8) The provider ensures that the integrated secure web-based management console has over a 99.5% uptime and support hours of 24x6, Sunday through Friday for all Internet-facing security devices.

Enterprise Intrusion Prevention / Detection Services (IPS/IDS)

C-9) Provide Traffic Visibility appliances. While service provider manages the appliances, OIM reserves the right to request changes to appliance configuration.
C-10) Provide Next Generation Firewall (NGFW) intrusion prevention/detection capabilities/devices at the perimeter firewalls.
C-11) Manage the filters or blocks to control unauthorized data sources and update existing filters and add new filters as updates become available. Ensure that each IPS/IDS filter exception submitted includes a detailed history of who (contact information) authorized the exception, the date that the exception was submitted, the reason for the exception, and the change request number.
C-12) Manage automated exchange capabilities between the IPS/IDS service and other security monitoring capabilities with OIM
C-13) Provide reputation/threat-based services/self-learning perimeter defenses, i.e., web application firewall, deep packet inspection including SSL, and Distributed Denial of Service (DDOS) reporting.

Web Content Filtering

C-14) Provide a Web Content Filtering (WCF) solution and reporting for all OIM's endpoints devices. This process should be approved by OIM.
• Make sure Web Content Filtering (WCF) solution has an enterprise global policy with agencies to have more restrictive policies.
• Web Content Filtering (WCF) reporting service shall provide long-term retention to generate viewable reports – both scheduled and/or on-demand.
C-15) Provide content filtering for mobile devices.

Security Threat and Vulnerability Assessment Services

C-16) Provide quarterly security threat and vulnerability identification, assessment and compliance management services for OIM
C-17) Manage automated data exchange integration capabilities with other SOC security equipment, through an independent third party, and include vulnerability identification and assessment, with the OIM's Governance, Risk and Compliance (GRC) platform.
C-18) The provider shall provide ad hoc scans or sets of scans to support specific audit or assessment requirements.

Enterprise SOC Services

C-19) Maintain any and all relevant security certifications for the facility where SOC functions will be housed.
C-20) Allow OIM and/or its internal or external auditors to audit the facility where monitoring is performed on at least a yearly basis.
C-21) Provide a backup path to receive alerts if the primary path becomes inoperable.

Network Security Monitoring, Alerting and Analysis Services

C-22) Network Security shall alert designated OIM authorities of security concerns ASAP or within 15 minutes of detection so countermeasures may be taken.
C-23) Maintain a Security Information and Event Management (SIEM) system providing real-time and analysis of security data and interfacing with the OIM's security tools and existing SIEM. The SIEM system must provide the capability to:
• Collect data from a broad array of network and security devices
• Normalize, aggregate and correlate diverse security event data
• Log source data into actionable data
• Obtain high visibility into security related events
• Identify threats and patterns of suspicious activity in real-time
• Automate analysis and alerting via email and /or GRC platform
• Rapidly respond to security events
• Support the gathering and reporting of compliance data for governance and compliance
C-24) SIEM solution shall provide OIM-specific dashboards to assist in detecting patterns and outlier activities.
C-25) Manage all devices that comprise the SIEM platform including configuration management and rules updates to address OIM monitoring requirements.
C-26) Enterprise SOC shall coordinate with the OIM's security operations teams to provide an incident response capability to protect the OIM network infrastructure. This includes providing processes, procedures, tools, resources and other capabilities, as necessary, to detect, respond to and report security incidents/breaches.

Controlled Penetration Testing (CPT) Services

C-27) Provide a CPT Management Plan update every six months.
C-28) Submit a weekly CPT Progress and Status Report that describes, at a minimum:
• Updated testing schedules
• Progress status on each CPT
• Issues and actions taken to address each issue
C-29) Scan and test for common web application vulnerabilities.
C-30) Document any "critical, high or medium" severity vulnerabilities that cannot be exploited within the specified timeframe of the CPT engagement due to time constraints.

C-31) Notify the OIM within thirty (30) minutes of detection of critical or high security incident. Notification can be sent to predefined OIM service desk operations
C-32) Acknowledge within one (1) business day, via e-mail, receipt of any CPT engagement extensions or change requests requested by the OIM. All Change Requests will adhere to the OIM's Change Request Processes.

Enterprise-wide Network Visibility and Discovery Services
C-33) Inspect OIM network assets to identify and measure relationships between known and unknown external OIM and Service Provider's network assets.
C-34) Coordinate with OIM to implement recommendations for risk reduction based on analysis of security event metrics.

D - Service Management and Provisioning

D-1) Remote OS level access (RDP, SSH) for the virtual machine instances with ability to provision servers, storage, CPU, RAM, etc. without requiring any vendor interaction, monitoring and recording logs of actions as needed.

Service Accounts
D-2) Support for multiple users with a customized portal view for each.

Service Monitoring and Measurement
D-3) Visibility for the different types of services via dashboard or web based console with predefined SLAs for each of the offerings along with Business Continuity and Disaster recovery capabilities and Data isolation mechanisms.

E – Business Continuity and Disaster Recovery (BCDR) Services

E-1) Provide and identify the resources (staff and equipment) that will be committed to the OIM in the event of a disaster.
E-2) Provide an incident manager in the event of a disaster who will be immediately available.
E-3) Meet with the OIM on a scheduled basis for BCDR planning and to review risks, tasks, and update the BCDR plan. Execute BCDR exercise on a predefined interval. The exercise shall be coordinated with OIM to minimize impact on business processes. Provide OIM the opportunity to observe and/or participate in the BCDR exercise. Document and provide the BCDR exercise results to OIM with identified deficiencies and associated remediation plans.
E-4) BCDR shall cover any type of disaster and have maximum recovery time of 72 hours for basic services, and 96 hours for return to business as usual.
E-5) Provide an operational back-up Enterprise SOC.

F – Transition Services

F-1) The selected service provider is expected to replace current service provider's infrastructure services in a staggered transition approach as OIM is expected to provide continuing core services with stability and reliability to its stakeholders. During the transition phase, the selected service provider must be willing to operate in dual supported environments by leveraging support from internal and external stakeholders.
F-2) Transfer of the services in accordance with the transition plan agreed to by OIM and including a number of transition milestones
F-3) Perform the transition without disruption to OIM's operations, and assume responsibility for all costs associated with the transition
F-4) The service provider's transition team shall meet weekly to discuss issues during transition. The service provider shall be responsible for agenda, meeting notes, etc. Meeting notes to be provided within three (3) days during the transition phase. The agenda, location and participants to be approved by OIM.
F-5) The service provider shall develop and maintain a Process and Procedures Manual which is available at all times to any authorized OIM staff.
F-6) Provide support for lift-and-shift, redeployment, and redevelopment of the existing services (Solaris,

UNIX, VMs, secure communication to our providers) used by OIM.
F-7) Provide support for migrating WordPress based website from either on-premise or cloud to cloud environment

G – (Optional) Provide IT Service Management (ITSM) tool

G-1) Provide an ITSM tool that can be used by UNJSPF/OIM as a ticketing system to manage incident/problems/change management and request fulfilment process, etc., This platform may be used by UNJSPF/OIM for the internal use for resolution workflows and can be used to escalate to service providers
G-2) Provide alignment with ITIL and ISO20000 standards.
G-3) Provide plans and implementation for multi-channel support, such as live chat boxes, automated voice calls, self-service, and self-diagnostics for users.
G-4) Provide integration with a Configuration Management Database (CMDB), with monitoring and reporting tools.
G-5) Provide capability for discovering, tracking and managing the service assets (infrastructure, security, applications, data, people, organization and IT knowledge)
G-6) Provide a method to discover applications and devices on the network to automatically update the CMDB.

Annex 1:

OIM currently has the following inventory of users, devices and services that requires monitoring in this service. The full CMDB and Services Catalog can be provided upon request:

i. Total number of users: 150
ii. Service Desk and Request fulfillers: 15
iii. Total Network Equipment (Firewalls (10), Access Switches (10), Routers (2), RSA Token (3), IronPort WSA (2): 27
iv. Total VMs: 30
v. Total Physical Servers: 1
vi. Microsoft Office 365 for email, one drive, SharePoint, skype for business, MS Teams etc.,
vii. Total Storage (Including Backup data and archives data): 200TB
viii. Data Protection Compliance: 7 years (2 years onsite and 5 years off-site)
ix. Website (https://oim.unjspf.org): 1
x. Desktops: 150
xi. Laptops: 100
xii. Handheld devices (tablets and phones) using IOS, Windows and Android: 250
xiii. Access Points: 10
xiv. Wireless Controllers: 3
xv. Printers: 10
xvi. Turret Trading Phones: 10
xvii. MS Azure: 2 servers currently in Test/Dev

**NOTE**

Information on tendering for the UN Procurement System is **available free of charge** at the following address: https://www.ungm.org/Public/Notice

Only the United Nations Global Marketplace (UNGM) has been authorised to collect a nominal fee from vendors that wish to receive automatically Procurement Notices or Requests for Expression Of Interest. Vendors interested in this Tender Alert Service are invited to subscribe on http://www.ungm.org

***Vendors interested in participating in the planned solicitation process should complete/submit the Vendor Response Form of this EOI either electronically (through the link available on the next page) or send it via fax or e-mail to United Nations Procurement Division (UNPD) before the closing date set forth above.***

# VENDOR RESPONSE FORM

**TO:** Joniolavi Kaerpijoki **EOI Number:** EOIJK717111

**Email:** joni.kaerpijoki@un.org

**FAX:**

**FROM:**

**SUBJECT:** Provision of Infrastructure-as-a-Service (IaaS) for UNJSPF

| NOTICE |
|---|
| • Companies can only participate in solicitations of the UN Secretariat after completing their registration (free of charge) at the United Nations Global Marketplace (www.ungm.org). |
| • As you express interest in the planned solicitation by submitting this response form, please verify that your company is registered under its **full legal** name on the United Nations Global Marketplace (www.ungm.org) and that your application has been submitted to the UN Secretariat. |
| • We strongly recommend all companies to register at least at **Level 1** under the United Nations Secretariat prior to participating in any solicitations. |

**PLEASE NOTE: You can express your interest to this REOI by filling out this form manually or electronically (recommended) at:**
https://www.un.org/Depts/ptd/node/add/interest-expressed?EOI=EOIJK717111

*To be completed by the Vendor (**All fields marked with an '*' are mandatory**)*

| COMPANY INFORMATION | |
|---|---|
| **UNGM Vendor ID Number*:** | |
| **Legal Company Name** (Not trade name or DBA name) ***:** | |
| **Company Contact *:** | |
| **Address *:** | |
| **City *:** | **State:** |
| **Country *:** | |
| **Telephone Number *:** | |
| **Fax Number *:** | |
| **Email Address *:** | |
| **Company Website:** | |

We declare that our company fully meets the prerequisites A, B, C, D, E and F, for eligibility to register with the United Nations as outlined in the paragraph 1 of the EOI INSTRUCTIONS page.

Signature :_____ Date:_____

Name and Title :_____

## EOI INSTRUCTIONS

### 1) Registering as a Vendor with the United Nations

Vendors interested in fulfilling the requirement described above must be registered at the UN Global Marketplace (**www.ungm.org**) with the UN Secretariat in order to be eligible to participate in any solicitation. Information on the registration process can be found at **https://www.un.org/Depts/ptd/vendors**.

**Prerequisites for Eligibility**
In order to be eligible for UN registration, you must declare that:

A. Your company (as well as any parent, subsidiary or affiliate companies) is not listed in, or associated with a company or individual listed in:

   I. the Compendium of United Nations Security Council Sanctions Lists (**https://www.un.org/sc/suborg/en/sanctions/un-sc-consolidated-list**), or

   II. the IIC Oil for Food List website or, if listed on either, this has been disclosed to the United Nations Procurement Division in writing.

B. Your company (as well as any parent, subsidiary or affiliate companies) is not currently removed or suspended by the United Nations or any other UN organisation (including the World Bank);

C. Your company (as well as any parent, subsidiary of affiliate companies) is not under formal investigation, nor have been sanctioned within the preceding three (3) years, by any national authority of a United Nations Member State for engaging or having engaged in proscribed practices, including but not limited to: corruption, fraud, coercion, collusion, obstruction, or any other unethical practice;

D. Your company has not declared bankruptcy, are not involved in bankruptcy or receivership proceedings, and there is no judgment or pending legal action against your company that could impair your company's operations in the foreseeable future;

E. Your company does not employ, or anticipate employing, any person(s) who is, or has been a UN staff member within the last year, if said UN staff member has or had prior professional dealings with the Vendor in his/her capacity as UN staff member within the last three years of service with the UN (in accordance with UN post-employment restrictions published in ST/SGB/2006/15.

F. Your company undertakes not to engage in proscribed practices (including but not limited to: corruption, fraud, coercion, collusion, obstruction, or any other unethical practice), with the UN or any other party, and to conduct business in a manner that averts any financial, operational, reputational or other undue risk to the UN.

**For Registered Vendors:** Vendors already registered at the UN Global Marketplace with the UN Secretariat must ensure that the information and documentation (e.g. financial statements, address, contact name, etc.) provided in connection with their registration are up to date in UNGM. Please verify and ensure that your company is registered under its full legal name.

**For Vendors Interested in Registration:** Vendors not yet registered should apply for registration on the United Nations Global Marketplace (**http://www.ungm.org**); information on the registration process can be found at **https://www.un.org/Depts/ptd/vendors**. Vendors must complete the registration process prior to the closing date of the REOI. Vendors who have not completed the UNGM registration process with the UN Secretariat before the closing date of the REOI are not considered eligible to participate in solicitations of the UN Secretariat. We strongly recommend all companies to register at least at Level 1 under the UN Secretariat prior to participating in any solicitations.

**IMPORTANT NOTICE: Any false, incomplete or defective vendor registration may result in the rejection of the application or cancellation of an already existing registration.**

### 2) EOI Process

Vendors interested in participating in the planned solicitation process should forward their expression of interest (EOI) to the United Nations Procurement Division (UNPD) by the closing date set forth in this EOI. *Due to the high volume of communications, UNPD is not in a position to issue confirmation of receipt of EOIs.*

Please note that no further details of the planned solicitation can be made available to the vendors prior to issuance of the solicitation documents.

This EOI is issued subject to the conditions contained in the EOI introductory page available at **https://www.un.org/Depts/ptd/eoi**.