TERMS OF REFERENCE
SECURITY LEAD
FOR THE MINISTRY OF HEALTH OF UKRAINE

ToR Date of Issuance:	**Mar 9, 2017**
Due Date for Applications:	**June 16, 2017**

PRSM is committed to providing equal employment opportunity without regard to race, color, religion, gender, sexual orientation, national or ethnic origin, age, disability or status as a veteran with respect to policies, programs, and activities.

Background

The Professionals for Reform Support Mechanism (PRSM) provides human resource support – from managers to technical experts - to critical reform initiatives undertaken by national governmental agencies. PRSM is a multi-donor platform, which improves coordination of donor efforts for greater impact and avoids overlap of donor funding. It does not support routine work of the Government of Ukraine that is normally managed by the civil service. To do this, PRSM: **Selects initiatives** based on clearly defined links to reform initiatives

- Ensures transparent **recruitment** of human resources
- Manages the **contracting** and payment of human resources
- Provides financial **reports** for donors
- **Monitors** initiatives for results.

Reform Initiative

The Ministry of Health of Ukraine has already announced the implementation of eHealth project as its priority. The Ministry seeks to establish a medical data system, which will maintain a pan-Ukrainian registry of patients, doctors and medical institutions, as well as possess data on contractual relations between them. The system will preclude healthcare actors from concluding fraudulent agreements, as well as provide invaluable statistics on diseases and prescribed treatment, which still do not exist in Ukraine to date. The Government of Ukraine (GoU) has a strong political will to launch eHealth solutions for the benefit of both its citizens and health care system. Political support has been well formulated by signing of 3 technical Memorandums by the Ministry of Health of Ukraine.

Position Summary:

Security Lead will be responsible for development of security model for eHealth and obtaining the CSIS (complex system of information security) certificate.

Preferred Qualifications and Skills:

- Bachelor degree in Computer Science, Information Systems or other related field;
- Minimum of 3 year of IT work experience with a board range of exposure to systems, application support, and/or database administration;
- Experience with information security;
- Knowledge of networking, Microsoft Windows desktop systems, Microsoft Windows Servers, Linux, Active Directory, Web Servers, Microsoft Exchange, Oracle DB, Web Application Firewalls and storage technologies;

- Strong technical background in information systems, systems administration, network design, network traffic analysis, and disaster recovery;
- Excellent problem solving skills Excellent communication skills, both written and oral;
- Ability to work with both team members and internal customers in a collaborative environment to provide security solutions that meet compliance requirements and project's needs;
- Ability to work with both team members and internal customers in a collaborative environment to provide security solutions that meet compliance requirements and project's needs;
- Applied knowledge of information security and compliance related issues involving PCI-DSS, PA-DSS, Sarbanes-Oxley, data privacy, and similar policies and laws;
- Fluent English and Ukrainian.

Indicative duties and responsibilities:

- Analyze and understand a variety of existing and emerging Line of Business application infrastructure requirements, perform risk analysis, and provide the technical leadership interface;
- Provides high level support and direction for production related issues;
- High Level design as it pertains to load balancing infrastructure and changes;
- Works with external vendors for chronic issues, bugs, feature enhancements;
- Review, revise and enforce policies and procedures that safeguard information systems and data from malicious, unauthorized or unintentional breach, loss, availability or performance degradation, or other compromise of computing assets;
- Responsible for maintaining IT Policies and Procedures;
- Participate in and ensure IT audits are completed in a timely manner;
- Coordinate data security log reviews in a timely manner and report on findings. Make recommendations for improvements;
- Perform semi-annual IT risk assessments;
- Provide project wide security alerts to known vulnerabilities;
- Stay current with the latest cyber security threat landscape and notify IT teams of applicability to the project's systems;
- Monitor third-party service providers for compliance with information security policies and procedures;
- Assess/quantify risk vs. cost with the ability to balance the likelihood/impact of real threats with costs of mitigation will be critical.

Contract Duration and Timing:
The total duration of the consultancy is expected to be 8 months, with possible extension, based in Kyiv.

To apply:
Submissions must be prepared in English and delivered electronically by 17:00 Kyiv time on June 16, 2017 to the following address: prsm@fsr.org.ua. We do not welcome unsolicited phone calls.
All submissions must include:

1) Applicant's CV (in English);
2) Applicant brief letter of interest indicated related experience and achievements.

Please ensure to state **Security Lead** in the e-mail subject line.

Applications received after the indicated deadline or without letter of interest will not be reviewed and considered.

Shortlisted candidates will be contacted after June 19, 2017.