**TERMS OF REFERENCE**

**for**

**Senior Advisor on Digital Reform and Establishment of the Office for Information Security**

1. **Background Information**

Digitalization is increasingly becoming the backbone of any and all functional restructuring in the public sector, an objective driver of change management and a precondition for transformative development. Going digital, being a horizontal measure, is also accelerating the attainment of Sustainable Development Goals (in further text: SDG). While it directly falls under SDG 16, e-Governance is contributing to building stronger institutions – effective, accountable and transparent – at all levels.

The Government of Serbia (GoS), elected in June 2017, has prioritized the digital transformation of the national economy and state administration. The Prime Minister's Keynote Address at the Parliament stressed digitalization and education as the most important catalysts of innovations, competitiveness and growth for Serbia in the coming years. It also stressed the need for a rapid digitalization of public administration and provision of integrated, secure and citizen-focused electronic services. This political support materialized in August 2017, when the new Government formed the Office for IT and e-Government (OITeG) and appointed the Prime Minister as head of the Council for Innovative Entrepreneurship and Information Technologies (IT Council).

In addition, the Government of Serbia has requested assistance from the World Bank in supporting the reform efforts, through a loan. To this effect, the World Bank has initiated the Enabling Digital Governance Project (EDGE). The Project, expected to be launched in April 2019, aims at contributing to development of the digitalization in Serbia, through implementation of the following components:

*Component 1: Foundations for Digital Service Delivery*

The objective of this component is to establish the necessary cross-cutting foundations to support the use of ICTs in the provision of public services to citizens, and businesses, including inter alia, regulations, standards, and digital infrastructure.

*Component 2. Citizen-Centric Digital Services*

The objective of this component is to support the three dimensions of project objectives—access, quality, and efficiency of e-services: (a) integrate change management and citizen engagement activities into this digital transformation process; (b) strengthen the institutional capacity of the OITeG and other key stakeholders for leading and coordinating intergovernmental activities in an agile, user-centric way; and (c) streamline the implementation arrangements through a partnership between OITeG and Public Policy Secretariat (PPS) of the Prime Minister’s office.

*Component 3. Digital Skills Development and Project Management*

This component focuses on the integration of change management, communication, and citizen feedback into Component 2.

For the purposes of effectively managing and coordinating EDGE and future Projects with International Financial Institutions (IFI) financing, the Project Implementation Unit (PIU) has been founded at the OITeG.

The Growth Plan for the Western Balkans was adopted by the European Commission on November 8, 2023, for the period 2024-2027. Based on the abovementioned Plan (sub-area: “Green and digital transition – Digitalization”, reform: “Setting up a comprehensive framework for cyber resilience and artificial intelligence”) the OITEG has a mandate to commence the establishment of the Office for Information Security (in further text OIS).

1. **Objective**

The goal of this engagement is to provide guidance on the team requirements for establishment of the Office for Information Security, as well as the procedural and legal framework requirements that are to govern the institution to be established.

1. **Scope of Work**

The duties of the Senior Advisor on Digital Reform and Establishment of the Office for Information Securityshall include, but are not limited to:

* Providing proposal of the organizational structure of the OIS;
* Definition of the criteria for selecting employees of the OIS , outlining specific set of skills and requirements;
* Providing more detailed analysis of the roles and responsibilities of employees within the OIS;
* Support organizational structure and development and maintenance of internal procedures prior and post establishment of the OIS
* Proposing a cooperation model between the OIS and the private sector, non-governmental organizations, and academic institutions;
* Providing proposals for establishing national legal entities aligned with the NIS2 Directive;
* Developing frameworks in line with the NIS2 Directive (e.g., Coordinated Vulnerability Disclosure Framework, Crisis Management Framework);
* Providing proposals for establishing National and Governmental CERTs in accordance with NIS2 requirements;
* Provide insight in design and implementation of trainings and professional development programs for individuals working in OIS, with a strong focus on information security, in collaboration with competent authorities and stakeholders from the public, academic, business, and NGO sectors;
* Engaging in national and international cooperation in the fields of digitalization, information security, and artificial intelligence;
* Proposing activities to enhance cyber incident response capabilities, especially through the planning of relevant exercises and training programs;
* Analyzing information on cyber threats, vulnerabilities, and both avoided and realized cyber incidents;
* Providing inputs to awareness raising campaigns among citizens, businesses, and public institutions about the importance of information security;
* Contributing to and developing design systems to ensure consistency and scalability across platforms;
* Suggest structures for oversight, reporting, and accountability within the OIS.
* Propose KPIs to assess the effectiveness of the OIS post-establishment.
* Provide guidance on long-term sustainability, including funding models.

The work of the consultant shall be summarized in the reports defined within the section “d”.

1. **Deliverables**

|  |  |  |
| --- | --- | --- |
| **No.** | ***Deliverable*** | ***Deadline*** |
| 1. | Readiness assessment on the establishment of the OIS (Office for Information Security) with envisaged organizational structure and systematization of work places within the OIS within the OITEG  | 40 days upon contract signing |
| 2. | Report on proposed operational plan for the OIS in the first year of operations | 80 days upon contract signing |
| 3. | Report on the proposal of internal procedures of the OIS | 110 days upon contract signing |
| 4. | Report on identified major public stakeholders essential to the work of OIS | 150 days upon contract signing |
| 5. | Report on identified major private stakeholders essential to the work of OIS | 180 days upon contract signing |
| 6. | Report on the first operational quarter of the OIS with proposal of the corrective measures | 210 days upon contract signing |
| 7. | Roadmap for OIS development of until December 2026 | 230 days upon contract signing |

1. **Reporting requirements**

The Consultant will work under the overall supervision of the OITEG Director.

1. **Length of assignment**

The Consultant shall provide part-time services under lump sum Contract paid upon acceptance of deliverables. The Consultant shall perform the Services until the Closing Date of the Project is May 31, 2026.

1. **Facilities to be provided to the Consultant**

OITEG will provide the Consultant with suitable office space and office equipment (PC, telephone, internet connection, etc.) and access to office services as required.

1. **Confidentiality**

The Consultant undertakes to maintain confidentiality on all information that is not in the public domain and shall not be involved in another assignment that represents a conflict of interest to the prevailing assignment.

1. **Qualifications**

In order to be selected, the Consultant must possess, at the minimum, the following qualifications:

* Bachelor’s degree in information technologies, electrical engineering, or a related field;
* Possession of an international certificate in cybersecurity is preferable;
* Experience in organization and management;
* Experience in implementing procedures and business solutions;
* Experience in creating and implementing an academic program for the education, training; and professional development of individuals working in digitalization is preferable;
* Experience in cooperation with state or private institutions in defining and implementing training or academic programs for the education of individuals involved in the implementation of information technologies in the public sector, is preferable;
* Experience in assessing the quality of education, training, and professional development programs for individuals working in digitalization is an asset;
* Participating in domestic and international projects;
* Good knowledge of written and spoken English and Serbian.
1. **Selection of the Consultant**

A Consultant will be selected in accordance with the Open Competitive Selection of Individual Consultants as set out in the WB Procurement Regulations for IPF Borrowers (July 2016, Revised November 2017 and August 2018).

The evaluation criteria for this assignment are:

• Specific Experience relevant to the Assignment (60) Points)

• Qualifications and Competence relevant to the Assignment (40) Points).

**Conflict of Interest**

The engaged Consultant must not be involved in any other related activity to this Project.