

Procurement Notice

Assignment name: Senior Expert for Penetration Testing and Security Assessment in the Agency for Identification Documents, Registers, and Data Exchange of Bosnia and Herzegovina

Reference Number: #22918

Section 1. Introductory Information

1.1 Background information on the Regional School of Public Administration (ReSPA)

The Regional School of Public Administration (ReSPA) is the inter-governmental organization for enhancing regional cooperation, promoting shared learning and supporting the development of public administration in the Western Balkans. ReSPA Members are Albania, Bosnia and Herzegovina, Macedonia, Montenegro and Serbia, while Kosovo* is a beneficiary. ReSPA's purpose is to help regional governments develop better public administration, public services and overall governance systems for their citizens and businesses and prepare for membership in the European Union.

ReSPA establishes close cooperation with ministers, senior public servants and heads of function in Member countries. ReSPA also works in partnership with the European Union, specifically Directorate General for Neighborhood and Enlargement Negotiations (DG NEAR), other regional players such as OECD/SIGMA and Regional Cooperation Council (RCC), as well as agencies and civil society organizations. Since its inception, ReSPA, as an international organization and a key regional endeavour in Public Administration Reform, has contributed to capacity-building and networking activities through in-country support mechanisms, peering and the production of regional research material.

The European Commission (EC) provides directly managed funds for the support of the ReSPA activities (research, training and networking programmes) in line with the EU accession process. So far, three EC Grant Contracts (GCs) have been implemented by ReSPA from the period 2010-2018. The current EC grant supports the implementation of the activities required for contribution to the achievement of the three strategic objectives during the period 2019-2021.

ReSPA works primarily through regional networks, which operate at three levels: Ministerial, Senior Officials, and networks/working groups of experts and senior practitioners. There is one network – Programme Committee composed of the representatives of institutions in charge of PAR, Public Financial Management (PFM) and government policy planning and the European Integration (EI) co-ordination process and five Working groups: (1) Centre-of-Government Institutions; 2) Better Regulation; 3) Human Resource Management and Development; 4) E-Governance; and 5) Quality Management.

ReSPA is implementing its activities through the Secretariat, which consists of 15 staff members from the Western Balkan region. The Secretariat is located in Danilovgrad, Montenegro.

1.2 ReSPA now seeks to engage one expert to provide support in the area of e-Government.

1.3 Expected deliverables of the assignment are: as per Terms of Reference.

1.4 Tentative timeframe: the assignment is expected to be performed during period **October – November 2022**.

1.5 **NOTE: Please, clearly indicate in the Methodology that you shall submit the entity with whom the contract would be concluded (in case your application will result successfully), i.e. whether the contract would be concluded with:**

- the expert as a physical person;
- a company on behalf of the expert (the name of the company should be also provided).

This cannot be changed in the procedure to follow.

In addition, you are kindly requested to fill and submit the following documents:

- Legal Entity File (for an individual expert) - https://ec.europa.eu/info/sites/default/files/about_the_european_commission/eu_budget/legent_indiv_en.pdf
- Legal Entity File (for a private company) - https://ec.europa.eu/info/sites/default/files/about_the_european_commission/eu_budget/legent_privcomp_en.pdf

Please, also submit any supporting documents required in these templates.

Section 2. Preparation of CVs and supporting documentation

2.1 Language of application:

The CVs and supporting documentation shall be prepared in English.

2.2 The CVs should provide information on the qualifications and competencies of the applicant, her/his general track record and previous specific experience in similar assignments, as required by the Terms of Reference. The applicants should particularly state in their CVs:

- Length of general and specific professional experience, in line with ToR;
- Professional experience in the role of lecturer/presenter.

2.3 The required qualifications, experience and skills: as per Terms of Reference

Section 3. Submission of CVs and supporting documentation

3.1 The interested candidates are invited to submit a proposal consisting of the following documentation:

- Proposal: explaining their experience related to the analysis subject and how they intend to respond to the assignment;
- Personal CV including past experience in similar activities and particularly issues referred to under point 2.2 of this Procurement Notice;

- At least three contacts for references (name and position of referee, email address and phone number) which may be contacted by ReSPA. (NOTE: There is no need to submit reference letters; ReSPA will directly contact the referees).

3.2 The required documentation should be submitted in electronic format by e-mail to the following address: procurement@respaweb.eu by **21 September 2022** before 2 PM CET. Late submissions will not be considered for evaluation. The application should contain in the e-mail title the following reference: **22918 Senior Expert for Penetration Testing and Security Assessment in the Agency for Identification Documents, Registers, and Data Exchange of Bosnia and Herzegovina**

Public servants from ReSPA Members and Kosovo* are not eligible to apply.

Selection 4. Evaluation of offers

4.1 The offer will be evaluated against the required qualifications, experience, skills and competencies as defined in the Terms of Reference.

4.2 The applicant securing the highest final ranking will be invited to submit a financial proposal (the financial proposal shall specify a total sum amount in EURO for the expert's daily fee) and negotiate the contract. If negotiations are successful, the selected candidate will be awarded the contract. Should the negotiations fail, the next ranked candidate will be invited to negotiations.

Section 5. Final Considerations

5.1 The payment will be done in one instalment, following the submission and approval of the deliverables.

5.2 The following document is attached to this Procurement Notice: Terms of Reference

5.3 ReSPA reserves the right to cancel this procurement procedure at any moment without any compensation to the applicants. The cost of preparing a proposal and negotiating a contract, including any related travel, cannot be reimbursed by ReSPA under any circumstances, nor can ReSPA be held liable for it, regardless of the outcome of the procurement procedure.

5.4 Should you need any further clarifications with respect to this procurement notice, please contact Ms Olivera Damjanovic, Programme Manager, via e-mail at o.damjanovic@respaweb.eu by **19 September 2022** (midnight) at the latest. ReSPA will post the response, including an explanation of the query without identifying the source of inquiry, on its website (www.respaweb.eu) by **20 September 2022**. Any request for clarification must be sent by standard electronic communication to the above e-mail address.

Terms of Reference

Request for Services

Senior Expert for Penetration Testing and Security Assessment in the Agency for Identification Documents, Registers, and Data Exchange of Bosnia and Herzegovina

1. Background

The Regional School of Public Administration (ReSPA) is the inter-governmental organization for enhancing regional cooperation, promoting shared learning, and supporting the development of public administration in the Western Balkans. ReSPA Members are Albania, Bosnia and Herzegovina, Macedonia, Montenegro and Serbia, while Kosovo* is a beneficiary. ReSPA's purpose is to help governments in the region develop better public administration, public services and overall governance systems for their citizens and businesses and prepare for membership in the European Union.

ReSPA establishes close cooperation with ministers, senior public servants and heads of function in Member countries. ReSPA also works in partnership with the European Union, specifically Directorate General for Neighbourhood and Enlargement Negotiations (DG NEAR), other regional players such as OECD/SIGMA and Regional Cooperation Council (RCC), as well as agencies and civil society organizations. Since its inception, ReSPA, as an international organisation and a key regional endeavour in Public Administration Reform, has contributed to capacity-building and networking activities through in-country support mechanisms, peering and the production of regional research material.

The European Commission (EC) provides directly managed funds for the support of the ReSPA activities (research, training and networking programmes) in line with the EU accession process. So far, three EC Grant Contracts (GCs) have been implemented by ReSPA from the period 2010-2015. The current EC grant supports the implementation of the activities required for contribution to the achievement of the three strategic objectives during the period 2019-2021.-

ReSPA works primarily through regional networks which operate at three levels: Ministerial, Senior Officials, and networks/working groups of experts and senior practitioners. There is one network – Programme Committee composed of the representatives of institutions in charge of PAR, Public Financial Management (PFM) and government policy planning and the European Integration (EI) coordination process and five Working groups: (1) Centre-of-Government Institutions; 2) Better Regulation; 3) Human Resource Management and Development; 4) E-Governance; and 5) Quality Management.

2. Description of the Assignment

The Agency for Identification Documents, Registers, and Data Exchange of Bosnia and Herzegovina (IDDEEA) based in Banja Luka, Bosnia and Hercegovina is responsible for digital signing in the field of identification documents, i.e. it is responsible for electronic certificates and electronic signatures related to identification documents, following the law governing the electronic signature. IDDEEA is also responsible for the cooperation with international institutions in charge of the field of identification documents.

The process of issuing electronic ID cards in BiH started on March 1st 2013. The Law on the Agency for Identification Documents, Registers and Data Exchange of Bosnia and Herzegovina ("Official Gazette of Bosnia and Herzegovina" No. 56/08) provides that the IDDEEA is responsible for the personalization and technical processing of identity cards and is responsible for digital signing in the field of identification documents. This means that IDDEEA is in charge of electronic certificates and electronic signatures related to identification documents, in accordance with the law governing electronic signatures.

In 2020, the Agency initiated many activities related to registration in the register of accredited verifiers in Bosnia and Herzegovina. According to the current regulations in Bosnia and Herzegovina, the Ministry of Transport and Communications of Bosnia and Herzegovina registers institutions in the register of verifiers, based on the previously completed process of CA certification by the competent certification body in the EU. IDDEEA has been successfully signed in the Register of Accredited Verifiers maintained by the Ministry of Communications and Transport of Bosnia and Herzegovina on 15th April 2022.

After the completion of the certification, IDDEEA fulfilled all legal preconditions to start the entry of the appropriate certificates for digital presentation and digital signing in the memory element of the identity card of the citizens of Bosnia and Herzegovina.

According to EU Regulation No. 910/2015 EIDAS and the audit conducted on 30 September 2021, all equipment, services and processes in IDDEEA intended for the issuance of qualified certificates fully meet the standards and measures envisaged by the abovementioned regulation. Practically, now as IDDEEA is entered in the register of verifiers, it can issue qualified certificates on the identity card of citizens of Bosnia and Herzegovina (electronic signature) which will be fully recognized in legal transactions in Bosnia and Herzegovina and outside Bosnia and Herzegovina.

The IDDEEA's system includes Public Key Infrastructure (PKI) necessary to support the Certification Authority. Smart cards and optionally biometrics are widely used for secure log-on and digital signature procedures. The system is fully compliant with the latest European Union directives and in accordance with EIDAS as well. Still, it is needed to make a risk analysis of the IDDEEA PKI to ensure the needed level of security. The assessment and identified measures from the Assessment Report will be implemented regularly and will have a positive impact on the level of security of the cyber ecosystem in Bosnia and Herzegovina.

In accordance with EIDAS and ISO 27001, IDDEEA needs to conduct regular penetration and vulnerability tests (PEN tests), for which IDDEEA should have internal capacities, i.e. sufficient in-house expertise within employees who will be able to conduct those tests regularly.

Such specific expertise is not available in IDDEEA and the training of selected public officials is needed. The knowledge and needed expertise that employees will gain through the training will be used for future testing and for improving the security of other parts of the information system, which is fundamental for future recertification. The trained employees will be able to conduct PEN tests independently (utilize adequate software, use technical documentation, and create reports). Team of the employees from IDDEEA who will be trained consists of 4 employees working on security on the IDDEEA network. IDDEEA will invite the officials from the BiH Tax office to join them and attend the whole training.

The expertise will raise the security level of IDDEEA's PKI and will boost the security of IDDEEA's information systems. The increased security level of IDDEEA's PKI will impact the level of security of the cyber ecosystem in Bosnia and Herzegovina.

With this document ReSPA is seeking a Senior expert to make the risk analyses of IDDEEA PKI and identify possible measures for improvement, conduct penetration and vulnerability tests (PEN tests), train the officials of IDDEEA (and invited officials from the BiH Tax Office), conduct PEN tests and provide the written recommendations for future testing and the Guidelines for conducting PEN tests.

3. Tasks and responsibilities

The Senior Expert will perform the following tasks with specified time allocations:

1. Do the risk Analysis of EIDAS PKI requirements and prepare the Assessment Report (2 days).
2. Prepare for facilitating the PEN tests and draft the Preparation report that will include the methodology and necessary steps and tools for testing (3 days).
3. Conduct the PEN tests and provide the output dataset. (5 days).
4. Draft the Final report following relevant standards for reporting and include in the Report written Guidelines for conducting the PEN tests. (5 days)
5. Conduct the five-day training for the group of four IDDEEA employees and invited officials from the BiH Tax office in Banja Luka. (5 days)

The assignment foresees the engagement of the Expert in cyber security for up to 20 (twenty) working days.

Additionally, ReSPA allows 1 additional day for the task of writing the Report with recommendations that also include specific recommendations related to possible regional replication.

In total, the assignment foresees the expert engagement of up to twenty-one (21) working days.

4. Necessary Qualifications

Qualifications and skills:

- At least Bachelor's Degree (4 years) or Master's Degree (3+1) in Information Technology, ICT, Computer Science, Information Science or equivalent;

General professional experience:

- Minimum of 3 years or more experience in the information security industry
- Minimum one similar project implemented.
- Adequate certificate for penetration tests (e.g. OSCP PEN – 200 or equivalent)

Specific professional experience:

- The consultant must have experience in information systems and information security
- Ability to write detailed documentation for both technical and non-technical audiences
- Excellent analytical skills as well as written and oral communication skills in English, desirable knowledge of Bosnian/Serbian/Croatian;
- Ability to provide training on the main topic of expertise.

Skills:

- Ability to write clear and coherent guidance documents;
- Ability to work with people of different nationalities, religions and cultural backgrounds.
- Training skills and moderation skills;
- High presentation skills.

5. Timing and Location

The assignment foresees work on location and exceptionally if the pandemic situation requires (official measures by the host country) work from home and provision of training in the online modality.

The assignment will be performed during October and November 2022.

6. Remunerations

One contract will be concluded. The payment will be done in one installment.

- Note: No other costs will be covered apart from the expert cost per day.

ReSPA reserves the right to change the timing and volume of the assignment and will timely inform assigned experts if such changes occur.

7. Reporting and Final Documentation

Outputs

- Assessment Report on the PKI risk assessment,
- Preparation report,
- Final report on PEN tests done with included Guidelines for conducting the PEN tests,
- Design and delivery of five-day training.

Documents required for payment from both experts:

- Invoice (signed original);
- Timesheets
- Report on the activity