REQUEST FOR EXPRESSIONS OF INTEREST
(REoI# MF-IC-15)
(CONSULTING SERVICES – INDIVIDUAL CONSULTANT)

UKRAINE

STRENGTHENING PUBLIC RESOURCE MANAGEMENT PROJECT, PART B: SUPPORT TO PFM STRATEGY IMPLEMENTATION (PROJECT NUMBER P161586)

Grant No. TF0A5324

Assignment Title: Information Cybersecurity Consultant for the Public Financial Management System Cloud

Reference No. MF-IC-15

The Government of Ukraine has received financing from the World Bank acting as administrator of the grant funds provided by the European Commission on behalf of the European Union under the EC - World Bank Partnership Program for Europe and Central Asia Trust Fund (EU Programme for the Reform of Public Administration and Finances (EURoPAF) toward the cost of the Strengthening Public Resource Management Project, and intends to apply part of the proceeds for consulting services.

The Ministry of Finance of Ukraine ("MoF") is responsible for the implementation of Part B of the Project and, to strengthen its capacity with regard to Project implementation, involves through competition an individual consultant - Information Cybersecurity Consultant for the Public Financial Management System Cloud (hereinafter – the Consultant) for conduction of organizational and technical activities on development and implementation of a comprehensive information protection system within the information and telecommunication system of MoF.

The consulting services ("the Services") include support to MoF in frames of the stages of the process of development and creation of a comprehensive information protection system ("CIPS") of the MoF Information and telecommunication system ("ITS") on the following:

1) Conduction of pre-project study (evaluation) of the operational environment of MoF ITS, the State Customs Service of Ukraine, the State Tax Service of Ukraine, the State Treasury Service of Ukraine for inclusion of the resources of the mentioned bodies into the common PFM cloud;
2) Working out the ITS information security policy for data processing technological processes in the common PFM cloud;
3) Design of ITS CIPS of the common PFM cloud and CIPS preparation for commissioning.

The evaluation is to reveal possible main gaps in information security, risks connected with them, and to propose measures on improvement of the situation.

It is expected that the evaluation will comply with both ISO 27001 and the relevant DSTU standards in terms of evaluation of information security maturity in each evaluated environment with the purpose of working out the action plan for transfer to creation of the common PFM cloud.

The Services are to be rendered at Consultant`s place of residence.
The Consultant is expected to work throughout the period from November 2020 to March 2021. The expected working time spent generally shall not exceed 120 working days.

More detailed information is stipulated in the ToR which is attached.

The MoF now invites eligible individual international consultants – physical persons ("Candidates") to indicate their interest in providing the Services in the form of CV (in Ukrainian or English). Interested candidates should provide information demonstrating that they have the required qualifications and relevant experience to perform the Services.
The candidates shall provide confirmation in the form of references to publicly confirmed and accessible information, or provide copies of relevant documents confirming the respective status or condition.
Interested Candidates are invited to submit any supplementary documents to evidence that Candidate meets with the qualification criteria for the position of the Consultant.

Mandatory qualification of the Consultant:

- higher technical education;
- at least 5 years of experience in the field of information protection, of which at least 2 years in the course of the last 5 years;
- availability of a qualification improvement certificate in technical and cryptographic protection of information, at least one certificate per each of the fields;
- experience in building up CIPS and preparation of documents for conduction of state expertises in the field of information technical protection within the last 5 years, with at least 3 implemented contracts/projects;
- knowledge and skills on practical application of the main Microsoft services, network services (DNS, DHCP, VLAN, VPN);
- experience of work with means of network security;
- fluent speaking and writing in Ukrainian.

The attention of interested Candidates is especially drawn to additional Consultants qualification requirements corresponding to the peculiarities of the assignment, meeting them would be an advantage:

- availability of a certificate of CISSP (Certified Information Systems Security Professional) or CISA (Certified Information Systems Audit) or CISM (Certified Information Systems Manager)
- availability of a certificate on successful completion of the training / training course on implementation and usage of the requirements of ISO / IEC 27001:2013 "Information Technology. Security Techniques. Information Security Management Techniques. Requirements" according to field of training "Implementor" and/or "Auditor";

- experience in implementation of comprehensive systems of protection of various types of information (AC1, AC2, AC3);
- availability of a scientific degree in technical sciences;
- availability of author patents for developments in information technical protection and comprehensive information protection;
- availability of a license from the State Service of Special Communication and Information Protection of Ukraine for performance of economic activity on rendering services in information technical protection;
- experience in CIPS build-up and preparation of documents for holding state expertises in information technical protection for public sector organizations;
- knowledge of English on a sufficient level for working through IT technical documentation without a dictionary.

The attention of interested Candidates is drawn to Section III, paragraphs, 3.14,3.16, and 3.17 of the World Bank's "Procurement Regulations for IPF Borrowers", July 1, 2016 with revisions as of November 2017 and August 2018"("Procurement Regulations"), setting forth the World Bank's policy on conflict of interest.

A Consultant will be selected in accordance with the Selection of Individual Consultants method (IC) set out in the Procurement Regulations.

Interested Candidates may obtain further information at the address below during office hours: 10:00 to 18:00.
Contact person: Volodymyr Vorotyuk
Tel: +38 044 206 5773, 380 50 4100340
E-mail: vorotyuk@outlook.com

Expressions of interest must be delivered by mail, fax or e-mail to the address below by 5 pm on November 4, 2020.

For EoIs submission:
Ministry of Finance of Ukraine
Attn: Mr. Igor Shevliakov, Head, Expert Group for EU Integration, Directorate for Strategic Planning and European Integration
The letter subject is – "Expression of interest on - MF-IC-15, Information Cybersecurity Consultant for the Public Financial Management System Cloud"
E-mail: shevliakov@minfin.gov.ua mandatory copy to: vorotyuk@outlook.com.

Attachment to REoI # MF-IC-15

TERMS OF REFERENCE

for provision of consulting services:

Information Cybersecurity Consultant for the Public Financial Management System Cloud

(Individual consultant)

Contract reference No.: MF-IC-15

1. BACKGROUND INFORMATION

The Government of Ukraine has received financial assistance from the International Bank for Reconstruction and Development ("World Bank"), acting as administrator of the grant provided by the European Commission on behalf of the European Union ("Donor") under the EC-World Bank Partnership Program for Europe and Central Asia Programmatic Single-Donor Trust Fund (EU Programme for the Reform of Public Administration and Finances (EURoPAF) three million thirty thousand six hundred sixty-one Euros (EUR 3,030,661) ("Grant") to implement the Strengthening Public Resource Management Project ("Project"). This Project consists of two parts: Part A "Strengthening Human Resource Management in Public Administration Institutions"; and Part B "Support to PFM Strategy Implementation".

Part B of the Project, total amount of which is one million one hundred ten thousand six hundred eighteen Euros (EUR 1,110,618), supports the activities aimed at implementing the PFM Strategy for 2017-2020 and identifies future investments in ICT for PFM through carrying out the audit of ICT; modernization of existing ICT equipment for business continuity at the Ministry of Finance of Ukraine ("MoF"); and strengthening ICT system capabilities, etc.

To achieve the objective, one of the main tasks of the PFM Strategy is wide application of reliable IT solutions and automation of the existing processes in the field of public finance management with the purpose of minimization of human impact and related corruption challenges.

MoF is responsible for implementation of Part B of the Project and, to strengthen its capacity with regard to Project implementation, involves through competition an individual consultant - Information Cybersecurity Consultant for the Public Financial Management System Cloud (hereinafter – the Consultant) for conduction of organizational and technical activities on development and implementation of a comprehensive information protection system within the information and telecommunication system of MoF.

2. PROBLEM DESCRIPTION

Currently in Ukraine each state body and company must ensure maximum automation of their life processes, prompt interaction and information exchange in the course of managerial decision making.

Dependence of organization on information systems, which ensure its life processes, is causing serious risks with regard to protection of information resources processed by means of such information systems. Failure of such an information system or unauthorized interference into its operation may lead to disastrous consequences for both the organization and the country on the

whole. That is why, simultaneously with implementation of information systems (“IS”), large attention is drawn to their security, fault tolerance, and protection of information, which circulates within the systems.

The information and telecommunication system of MoF (“ITS”) constitutes a service-oriented hardware and software platform for implementation and fulfillment of typified applied information services, which are implemented based on a common hardware and software platform, support a common information processing technology, and ensure mechanisms for implementation of the provisions of the uniform security policy approved by MoF.

The ITS hardware and software platform implements the strategy of a common integration system, which comprises technologies and hardware enabling to sustain a functionally closed and self-sufficient data processing system in frames of created (implemented) applied services (automated systems), with support of specified fixed (for all ITSs) types of objects of protection, access subjects (user groups and roles), and basic operation conditions.

Under Article 6 of the Law of Ukraine "On Access to Public Information" and Article 21 of the Law of Ukraine "On Information", requirements are raised to information processed by means of information systems of the state bodies and stored in state registers, with regard to ensuring its confidentiality, integrity, and accessibility in the course of its processing.

In this case, under Order of the Cabinet of Ministers of Ukraine dated 10.07.2019 No. 594-r "On Approval of the Concept of IT centralization of Public Finance Management", creation of a uniform landscape of IT systems with a high level of integration and interaction is envisaged, which, in its turn, supposes usage of a common data storage with up-to-date information.

Implementation of usage of a common data storage can be ensured through creation of a common cloud (a territorially distributed data processing center) of MoF, the State Customs Service of Ukraine, the State Tax Service of Ukraine, and the State Treasury Service of Ukraine (“the common PFM cloud”).

Usage of cloud services is not only convenient, but also safe, because even if something happens with the hardware certain information is stored on, data will not disappear, because the essence of cloud technologies lies in moving data processing from computers to global network servers.

In Ukraine, this issue is not properly governed on the legislative level, thus there appeared the need in adoption of a document, which would govern such relations, as well as relations connected with data processing and protection in case of provision of cloud-based services, as well as ensure and govern the procedure of cloud services usage by state bodies.

Thus, on June 16, 2020, the Verkhovna Rada of Ukraine adopted in the first reading Draft Law "On Cloud Services" No. 2655 dated 20.12.2019.

In this case, to ensure the ITS security policy in compliance with the requirements of the current legislation of Ukraine and to exclude or minimize losses caused by unauthorized access to information resources, a comprehensive information protection system (“CIPS”) shall be created, with confirmed compliance in accordance with Article 8 of the Law of Ukraine "On Information Protection in Information and Telecommunication Systems". Compliance shall be confirmed based on the results of the state expertise in the procedure set by the legislation.

The ITS CIPS shall be developed in accordance with the typical procedure of CIPS creation in automated systems (ND TZI 3.7-003-05), with account of the integrated approach to implementation of the components of its architecture.

The objective of creation of the ITS comprehensive information protection system is to ensure protection of information processed by means of the ITS, through prevention of and combating unauthorized access, disclosure, distortion, and loss of information during its processing and transmission. Information protection shall be ensured on all technological stages of its processing and in all functioning modes of ITS components. The CIPS is an integral part of the ITS.

The CIPS is a set of software and technical means as well as organizational activities, aimed at ensuring the established level of information protection in accordance with the conditions of ITS operation environments and requirements to ensuring the main security characteristics defined in the security policy of the System and the administrator organization. The ITS CIPS is designed for implementation of the information protection policy provisions with regard to:

- identification and authentication of System users during access to and usage of protected objects;
- management of authorized users and division of powers on usage of ITS information and software resources;
- ensuring confidentiality and integrity of information circulating within the ITS and/or transmitted between its components;
- ensuring identification and authentication of ITS units during an interaction session;
- ensuring confidentiality and integrity of information provided to external users/systems;
- ensuring identification and authentication of external systems' units during an interaction session;
- ensuring confidentiality, integrity, and accessibility of technological information on system functioning;
- ensuring accessibility of information circulating within the ITS, for authorized users and processes;
- registration and processing of all events within the ITS, related to information security;
- monitoring of the current status of security and operability of ITS components;
- control of all security mechanisms via the relevant administration interface, which shall be accessible only to authorized staff.

3. OBJECTIVES OF THE ASSIGNMENT

The objective of the assignment is rendering services in frames of the stages of the process of development and creation of the MoF ITS CIPS on the following:

- Conduction of pre-project study (evaluation) of the operational environment of MoF ITS, the State Customs Service of Ukraine, the State Tax Service of Ukraine, the State Treasury Service of Ukraine for inclusion of the resources of the mentioned bodies into the common PFM cloud;
- Working out the ITS information security policy for data processing technological processes in the common PFM cloud;
- Design of ITS CIPS of the common PFM cloud and CIPS preparation for commissioning.

The evaluation is to reveal possible main gaps in information security, risks connected with them, and to propose measures on improvement of the situation.

It is expected that the evaluation will comply with both ISO 27001 and the relevant DSTU standards in terms of evaluation of information security maturity in each evaluated environment with the purpose of working out the action plan for transfer to creation of the common PFM cloud.

The key technical aspects evaluation will be focused on, will include, among other things, the following:

1) documenting of systems (availability of instructions on deployment, installation, updating etc.), security policy and security procedure;

2) access control system and methodology: for evaluation of availability of access control means to prevent receipt, usage, or change of information by unauthorized users;

3) users' identification and authentication;

4) network security: data encryption, authentication services (including with usage of a qualified digital signature), and security protocols are utilized to assess whether firewalls are set up;

5) security infrastructure, including firewalls, intrusion prevention systems (IPS), security information and event management (SIEM), enterprise monitoring system (EMS);

6) organizational measures on registration and maintenance of distributed users;

7) security measures in terms of recording in protocols the actions of systems administrators.

4. SCOPE OF SERVIVCES AND TASKS

The Consultant shall perform the following tasks according to the stages below:

4.1 At the stage of pre-project study (evaluation) of the operational environment of MoF ITS, the State Customs Service of Ukraine, the State Tax Service of Ukraine, the State Treasury Service of Ukraine (for inclusion of the resources of the mentioned bodies into the common PFM cloud), the Consultant shall:

- Work out and submit for the Client's approval justified concept solutions on the levels of presentation of the architecture of MoF ITS of the common cloud, draft design and scenario of CIPS build-up in the ITS. Analyze the possibilities and need for implementation of organizational and technical solutions.
- According to the result of the provided data on the analysis of probability and consequences of potential threats to information in accordance with the defined ITS resources, technological processes of the system, and vulnerabilities of the hardware and software support of ITS components based on approved concept solutions on the levels of presentation of ITS architecture of all bodies (MoF, State Customs Service, State Tax Service, State Treasury Service), form the assignment to create and implement the ITS CIPS of the common PFM cloud:

  - determine the task of information protection within the ITS, purpose of CIPS creation, option of solution of protection tasks (in accordance with DSTU 3396.1), main directions for ensuring protection;

- conduct market analysis (study of the model of threats and the model of the breacher, possible consequences of implementation of potential threats etc.) and determine the list of significant threats;

- determine the overall structure and composition of the CIPS, requirements to possible activities, methods, and means of information protection, acceptable restrictions on usage of certain protection measures and means, other restrictions on ITS operational environments, restrictions on usage of ITS resources for implementation of protection tasks, acceptable costs for creation of CIPS, conditions of CIPS (its separate sub-systems, components) creation, commissioning, and operation, general requirements to the proportion and limits of application within the ITS (its separate sub-systems, components) of organizational, engineering and technical, cryptographic, and other measures on information protection, which will be included into the CIPS.

- Based on the results of the analysis, prepare the documents as per para. 1 of Section 5 of the present Terms of Reference.
- Preparer and submit the relevant report on pre-project study and amend it, if required.

4.2 At the stage of development of the information security policy of ITS of the common PFM cloud for technological processes of data processing and working out the Terms of Reference of CIPS creation within the ITS of the common PFM cloud, the Consultant shall:

- Work out and submit for the Client's approval the structure and concept of the Terms of Reference of CIPS creation within the ITS of the common PFM cloud, which, based on the above principal ITS architecture levels, shall include the following as separate documents and/or sections:
  - Terms of Reference for CIPS Software and Technical Complex of the central segment of the information and telecommunication system of the common PFM cloud;
  - Technical Specifications on the Organizational and Technical Solutions ("OTS") for implementation of protection activities and technologies for typical interfaces of user access to ITS information resources.
- Determine security objectives with regard to information and computing resources by each ITS architecture level, with account of the measures for reduction of the risks of implementation of threats, characteristics of operational environments and information processing technologies, proposed in the threats model.
- Determine the types of information objects containing ITS information and computing resources, describing/presenting access subjects, and being subject to protection in frames of information processing.
- Provide description of the security policy. All subjects, objects, operations, security attributes, and other terms used in (within) the ITS, shall be defined in frames of the provided security policy. The wording of the security policy in the Terms of Reference shall identify all protection requirements and activities, in accordance with information processing technological processes, system architecture, and determined scenarios and risks of threat activities.
- Determine the level of guarantees and requirements, which can be ensured by the Developer in the course of CIPS development and implementation. The level of

guarantees shall not be lower than G2, the requirements to which are specified in ND TZI 2.5-04-99.

- Based on the results of the analysis, prepare the documents as per para 2 of Section 5 of the present Terms of Reference.
- Prepare and submit the relevant report on development of the ITS information security policy and incorporate amendments to it, if required.

4.3 At the stage of design of CIPS of ITS of the common PFM cloud and CIPS preparation for commissioning, the Consultant shall:

- Develop the general design solutions required for implementation of the Terms of Reference requirements according to threat scenarios, solutions on the ITS CIPS structure, functioning algorithms, and conditions for usage of protection means.
- Work out the project of the architecture of the complex of ITS information protection means with account of the approved system levels and integrated system components.
- Form the assignment for working design of components and subsystems of the protection means and of the complex of information cryptographic protection in the ITS.
- Work out the project of ITS information security management organizational structure in accordance with the approved ITS CIPS architecture and with account of international and regional standards, which includes:
  - design solutions on the principal processes for ensuring information security management in the ITS with regard to the approved CIPS architecture and rules of its operation;
  - staff structure and work modes for the staff servicing the set of protection means and the information security protection system;
  - requirements to staff qualification levels, training programs.
- Based on the results of the design, prepare the documents as per para. 3 of Section 5 of the present Terms of Reference.
- Prepare the documents on the result of development of security policies and conduction of preliminary testing of ITS CIPS implementation, as specified in para 3 of Section 5 of these Terms of Reference.

- Prepare and submit the relevant report on creation of the CIPS design documentation and incorporate amendments to it, if required.

It is planned that the Consultant will perform the greater part of his/her work at the central site in MoF, where the infrastructure of the future common PFM cloud is located.

Additionally, the Consultant shall visit the State Customs Service of Ukraine, the State Tax Service of Ukraine, and the State Treasury Service of Ukraine for collection of information directly at locations where primary information is processed and accumulated.

The Consultant shall apply its own methodology for performance of the work.

The Consultant is expected to utilize various tools and technological components (including those of his/her own) for conduction of tests.

5. DELIVERABLES AND TIMING FOR THEIR PROVISION

The Consultant shall prepare and provide to MoF the following results[1]:

No.	Result	Deadline for submission *(from the date of contract signing)*
1	Report on pre-project study of the operational environment of MoF ITS, the State Customs Service of Ukraine, the State Tax Service of Ukraine, the State Treasury Service of Ukraine (for inclusion of the resources of the mentioned bodies into the common PFM cloud), including: • report on the results of risks analysis; • draft design and scenario of CIPS build-up in the ITS (to incorporate description of the threats model, breacher model, survey act, developed by another individual consultant) • information protection plan;	Within 80 working days
2	Report on development of the security policy of the ITS of the common PFM cloud and of the Terms of Reference for CIPS of the ITS of the common PFM cloud, including: • Text description on development of the Terms of Reference for ITS CIPS. • Terms of Reference for CIPS Software and Technical Complex of the central segment of the information and telecommunication system of the common PFM cloud. • Technical Specifications on the OTS for implementation of protection activities and technologies for typical interfaces of user access to ITS information resources.	Within 90 working days
3	Report on preparation of the technical project of the ITS of the common PFM cloud and CIPS preparation for commissioning, including: a. Design documentation of the technical detailed project of CIPS of the common PFM cloud: • Technical design schedule • Technical design text description. • Description of the organizational structure of ITS administration and operation b. Documentation on CIPS tests conducted: • Security policies' basic parameters set-up protocols c. CIPS supporting documentation:	Within 120 working days

1 The mix of deliverables and the timing of fulfillment of the assignment may be precised during the contractual negotiations with the Consultant, as per the proposed methodology of services rendering.

	• forms of registration logs.	

6. COORDINATION, ACCOUNTABILITY AND REPORTING

The Consultant shall work under the supervision of the Project Coordinator from the MoF and shall be accountable/report to him/her. All documents prepared by the Consultant, may further be included into the documents package, which will be approved on the level of a MoF regulatory act.

The Consultant shall coordinate his/her work with the MoF's IT Coordinator in terms of development of coordinated solutions for working through and building up a conceptual model serving as basis for the Strategy of Development of Information Technologies of MoF for the Years 2020-2022, and provide to MoF representatives output information on fulfillment of the assignment.

In the course of operational interaction, the Consultant shall be subordinated to the Lead Information CyberSecurity Consultant (individual consultant) and cooperate with

MoF specialized subdivision authorized with the functions of the information protection service.

Lead Information Cyber Security Consultant (individual consultant) is entitled to

- control the timing and quality of preparation of all Consultant's reports;
- provide (if any) comments to the documents attached to the Consultant's reports, check the fact of correcting these comments.

The Consultant shall prepare and submit to the MoF the following reports:

- Report on pre-project study of the operational environment of MoF ITS, the State Customs Service of Ukraine, the State Tax Service of Ukraine, the State Treasury Service of Ukraine (for inclusion of the resources of the mentioned bodies into the common PFM cloud);

- Report on development of the security policy of the ITS of the common PFM cloud and of the Terms of Reference for CIPS of the ITS of the common PFM cloud;

- Report on preparation of the technical project of the ITS of the common PFM cloud and CIPS preparation for commissioning;

1. The Consultant shall provide the Report on pre-project study of the operational environment of MoF ITS, the State Customs Service of Ukraine, the State Tax Service of Ukraine, the State Treasury Service of Ukraine (for inclusion of the resources of the mentioned bodies into the common PFM cloud) not later than the deadline set for result No. 1 in Section 5 of the present Terms of Reference. The report is to be prepared based on the results of tasks fulfillment and shall contain the following information:
    - information on the first stage of the works performance as per the list of documents provided in para. 1 of Section 5 of the present Terms of Reference;
    - problematic issues which the Consultant considers to be obstacles for timely and quality services rendering and proposed measures on elimination of such issues;
    - general information on readiness of the whole set of documents specified in para. 1 of Section 5 of the present Terms of Reference;
    - other information upon the Consultant's discretion.

The documentation prepared by the Consultant, as specified for Result No. 1 in clause 5 of the present Terms of Reference, shall be attached to the Report.

2. The Consultant shall submit to MoF the Report on development of the security policy of the ITS of the common PFM cloud and of the Terms of Reference for CIPS of the ITS of the common PFM cloud not later than the deadline set for result No. 2 in Section 5 of the present Terms of Reference. The report is to be prepared based on the results of tasks fulfillment and shall contain the following information:
    - general information on the second stage of the works performance;
    - design documentation for the CIPS technical detailed project as per the list of documents specified in para. 2 of Section 5 of the present Terms of Reference;
    - problematic issues which the Consultant considers to be obstacles for timely and quality services rendering and proposed measures on elimination of such issues;
    - general information on readiness of the whole set of documents specified in para 2 of Section 5 of the present Terms of Reference;
    - other information upon the Consultant's discretion.

The documentation prepared by the Consultant, as specified for Result No. 2 in clause 5 of the present Terms of Reference, shall be attached to the Report.

3. The Consultant shall submit to MoF the Report on preparation of the technical project of the CIPS of the ITS of the common PFM cloud and CIPS preparation for commissioning not later than the deadline set for result No. 3 in Section 5 of the present Terms of Reference. The report is to be prepared based on the results of tasks fulfillment and shall contain the following information:

    - information on readiness of the set of documents specified for result No 3 in of Section 5 of the present Terms of Reference;

    - design documentation for the CIPS technical detailed project as per the list of documents specified for result No 3 of Section 5 of the present Terms of Reference;

    - problematic issues which the Consultant considers to be obstacles for timely and quality services rendering and proposed measures on elimination of such issues;

    - other information upon the Consultant's discretion.

The documentation prepared by the Consultant, as specified for Result No. 3 in clause 5 of the present Terms of Reference, shall be attached to the Report.

4. Requirements to the reports

All reports are compiled in Ukrainian language. Any appendices to them shall be in the original language.

All reporting documents shall be submitted by the Consultant in the following manner:

- The Consultant shall submit the reporting documents in electronic form via email: _____ for review and comments by the MoF (reports shall be signed by the Consultant, scanned in pdf format and sent from Consultant`s e-mail indicated in para. 5 below). Supporting documents shall be in the MS Word, MS Excel or MS PowerPoint format or any other form previously agreed with or acceptable to the MoF, depending on the type of a document.

- If the MoF agreed reporting documents submitted via email, the Consultant shall submit them in paper form in 2 hard copies signed by the Consultant. The Paper version shall be submitted on the following address: Kyiv, 04071, Mezhegirska str., build. 11, Attn to Mr. Igor Shevliakov.

If the Consultant's report refers to information or documents prepared earlier, such documents shall be attached to such a report. The structure and form of the reporting documents specified in Section 5 of the present Terms of Reference, is determined by the requirements of regulatory documents of the information technical protection system.

5. Review and approval of the Reports

The MoF reviews the submitted reporting and approves or provides comments within 10 working days from the date of receiving the relevant report about the results of the work. The comments on the reports are set out in writing and sent to the Consultant via email: _____ with the notification of delivery of the message. The Consultant confirms the receipt of the comments and sets the deadline for their consideration within a day after receiving MoF's comments. The Consultant shall take into account the MoF's comments and re-submit updated report(s) MoF no later than within 5 working days from the date of their receipt to the e-mail, specified by the Consultant.

In the absence of the MoF's comments within the specified period, such reports are considered accepted.

7. CLIENT INPUTS

MoF provides the Consultant with:
i) all the relevant documents and data not marked as restricted access or not belonging to confidential information;
ii) access to the MoF premises.
iii) It is indicated above that a Consultant is to visit other institutions for data collection, so the MoF is to ensure the establishing needed contacts for the Consultant in such institutions

8. RESTRICTIONS

The Contract with the Consultant contains a standard conflict of interests clause. Apart from that, all materials created during performance of the services under the Contract, shall remain the property of MoF and may be used only upon the official written consent of MoF.

Prior to commencement of the services, the Consultant jointly with MoF shall prepare a confidentiality statement, where he/she shall undertake not to disclose the confidential information he/she can receive in the course of fulfillment of the assignment. The provisions of the confidentiality statement shall comply with the requirements of the current legislation of Ukraine.

9. PLACE, DURATION, WORKING CONDITIONS AND REMUNERATION

The Consultant is expected to work throughout the period from November 2020 to March 2021. The expected working time spent generally shall not exceed 120 working days. The assignment envisages the Consultant's work at his/her place of residence.

The amount of the remuneration will be determined through negotiations with the selected person and payment for the services provided will be made against reports accepted.

The Consultant is responsible for all costs incurred in connection with the provision of services, including, but not limited to the following: accommodation at the place of service, translation, communication costs, printed materials

The selection of consultant will be done in accordance with the Bank's "Procurement Regulations for IPF Borrowers", July 1, 2016 with revisions as of November 2017 and August 2018 ("Procurement Regulations").

10. QUALIFICATION REQUIREMENTS

The Consultant shall meet the following qualification requirements:

Mandatory qualification for the Consultant:

- higher technical education;
- at least 5 years of experience in the field of information protection, of which at least 2 years in the course of the last 5 years;
- availability of a qualification improvement certificate in technical and cryptographic protection of information, at least one certificate per each of the fields;
- experience in building up CIPS and preparation of documents for conduction of state expertises in the field of information technical protection within the last 5 years, with at least 3 implemented contracts/projects;
- knowledge and skills on practical application of the main Microsoft services, network services (DNS, DHCP, VLAN, VPN);
- experience of work with means of network security;
- fluent speaking and writing in Ukrainian.

Additional qualification requirements corresponding to the peculiarities of the assignment, meeting them would be an advantage

Meeting the following qualification requirements by the Consultant would be considered by the MoF as an advantage:

- availability of a certificate of CISSP (Certified Information Systems Security Professional) or CISA (Certified Information Systems Audit) or CISM (Certified Information Systems Manager)
- availability of a certificate on successful completion of the training / training course on implementation and usage of the requirements of ISO / IEC 27001:2013 "Information Technology. Security Techniques. Information Security Management Techniques. Requirements" according to field of training "Implementor" and/or "Auditor";
- experience in implementation of comprehensive systems of protection of various types of information (AC1, AC2, AC3);
- availability of a scientific degree in technical sciences;
- availability of author patents for developments in information technical protection and comprehensive information protection;

- availability of a license from the State Service of Special Communication and Information Protection of Ukraine for performance of economic activity on rendering services in information technical protection;
- experience in CIPS build-up and preparation of documents for holding state expertises in information technical protection for public sector organizations;
- knowledge of English on a sufficient level for working through IT technical documentation without a dictionary.

The candidates shall provide confirmation in the form of references to publicly confirmed and accessible information, or provide copies of relevant documents confirming the respective status or condition.