EUACI EUROPEAN UNION ANTI-CORRUPTION INITIATIVE

TERMS OF REFERENCE

Request for Bid
for Website Design, Development, and Implementation of the State Financial Monitoring Service of Ukraine (SFMS)

4 October 2018

This program is financed by the European Union
and co-financed and implemented by DANIDA

MINISTRY OF FOREIGN AFFAIRS OF DENMARK
Danida

1. LIST OF ABBREVIATIONS

AML/TF	Prevention and Counteraction to Legalization the Proceeds from Crime (Anti-Money Laundering), Terrorism Financing, as well as Financing Proliferation of Weapons of Mass Destruction
DBMS	Database Management Systems
DSTU	State Committee of Ukraine for Standardization, Metrology and Certification
FATF	Financial Action Task Force
FMSA	Financial Monitoring System Account
IIPS	Integrated Information Protection System
ISFM	Integrated System of Financial Monitoring in the AML/TF Area
CMS	Content Management System
OS	Operating System
SFMS	State Financial Monitoring Service of Ukraine
TCB	Trusted Computing Base
TPI	Technical Protection of Information
USPA	Ukrainian Sea Ports Authority

2. INTRODUCTION

Endemic corruption remains to be one of the major impediments for democratic and economic development of Ukraine.

Support of anti-corruption efforts in Ukraine is a high priority for Denmark and the rest of the EU contributing to the enhancement of democracy, as well as future economic growth and trade between Ukraine, Denmark and the rest of the EU Member States. The EU Anti-Corruption Initiative (hereinafter referred to as "EUACI") is the largest EU-supported programme in the area of anti-corruption in Ukraine so far. The overall objective of the EUACI is to improve implementation of anti-corruption policy in Ukraine, thereby ultimately contributing to a reduction in corruption.

EUACI is aimed at:

- strengthen the capacity of the newly created anti-corruption institutions;
- enhance external oversight over the reform process by the Verkhovna Rada;
- enhance the capacity of local government, civil society, and media to contribute to the fight against corruption.

Contracting Authority

The contracting authority is the European Union Anti-Corruption Initiative in Ukraine (EUACI), supported by the EU and Denmark and implemented by Danida, hereinafter referred to as the "Customer".

Beneficiary

The beneficiary is the State Financial Monitoring Service of Ukraine (SFMS). It is the central executive authority directed and coordinated by the Cabinet of Ministers of Ukraine through the Minister of Finance of Ukraine, that implements the state policy as the key element of the prevention and counteraction to legalization the proceeds from crime (anti-money laundering), terrorism financing, as well as financing proliferation of weapons of mass destruction (AML/TF). The SFMS, among others, is being supported by the EUACI within the first component.

Official Name and Symbolic Representation

Full name of the website of the State Financial Monitoring Service of Ukraine is "The official website of the SFMS of Ukraine" (hereinafter referred to as the "SFMS website" or "website").

3. OBJECTIVE

3.1 Application

The website is intended for promulgation of information on the activities of the State Financial Monitoring Service of Ukraine on the Internet in order to increase the efficiency and transparency of its activities, to provide information and other services to the public, to ensure its impact on the processes that take place in the AML/TF.

Under applicable law, the website provides the entities with access to information in the AML/TF area and is the official source of its provision.

3.2 Purpose of Development

The purpose of website development is to provide the following via the Internet:

- information about the SFMS activities on the implementation of the state policy in the AML/TF area;
- information in the AML/TF area from the SFMS to the entities;
- possibility of obtaining information by the entities in accordance with the legislation of Ukraine;
- adapting the information in the AML/TF area to mobile users and visually impaired people.

3.3 Target Audience of the Website

1) Entities that carry out activities in the AML/TF area:
   - primary financial monitoring entities;
   - state financial monitoring entities;
   - government authorities, organizations and other entities providing information in the AML/TF area;
   - the SFMS employees;
   - website administrators;
   - financial intelligence units from other states.
2) National and international organizations, public associations.
3) Other legal entities or individuals.

3.4 Hosting and Domains

Website consists of the following subsites:

fiu.gov.ua	The official website of the State Financial Monitoring Service of Ukraine
blind.fiu.gov.ua	The official website of the SFMS adapted for visually impaired people
m.fiu.gov.ua	The official website of the SFMS adapted for viewing on mobile devices
cabinet.fiu.gov.ua	The official website of the SFMS for the access to the Financial Monitoring System Account (FMSA) by the entities

3.5 List of Measures of Website Development

The following main tasks should be undertaken with regard to website development:

1) development of a website design that meets the W3C standards (https://www.w3.org/standards/webdesign);
2) creation of an official SFMS website;
3) creation of a custom website adapted for visually impaired users as well as an adaptation information module;
4) creation of a custom website adapted for the mobile devices;
5) creation of a website module for the public information accounting system;
6) creation of a search engine website module;
7) creation of a website module for electronic public appeals;
8) creation of a website module for email distribution;
9) creation of a feedback website module;
10) development of a website management system, a procedure for entry and dissemination of information (articles, photos, videos, etc.);
11) delivery and installation of the software required for the functioning of the aforementioned website components (systems) on the Beneficiary's hardware and software platform;
12) data migration from the old SFMS website to the new official SFMS website;
13) website integration into the Integrated System of Financial Monitoring in the AML/TF area (ISFM) and its Integrated Information Protection System (IIPS ISFM);
14) website testing.

4. SCOPE OF WORK

4.1 Website Requirements as a Whole

A website is a hardware and software system. The website is integrated into ISFM by placing virtual servers with the website software installed on its equipment.

4.2 Website Design Requirements

Information on the website is nested by the HTML programming language elements: headings, lists, tables, frames.

The structure of nested menu items should not exceed 3 levels.

All web pages should contain textual information on their location in the website hierarchical structure.

The first start page of the SFMS website should be static and contain relevant sections for reporting on the SFMS activities.

By navigating the website, the language switch tools, the search service, the SFMS hotline and an easy access tool to the website by visually impaired people should be sequentially located in the upper corner to the right.

By navigating the start page, the SFMS logo and the inscription "The official website of the SFMS" should be located at the bottom left alongside the above-mentioned services, and the Flag of Ukraine with the Coat of Arms of Ukraine should be located on the right.

By navigating the website, in parallel to the above-mentioned services, the following sections should be unblocked, horizontally centred, placed in a sequential and symmetrical order: «About the Service», «Documents», «Activity», «Coordination», «Methodology», «Academy», «Technologies», which according to the website structure contain relevant sections. To the right of these sections there should be an access banner to FMSA, and just below it, there should be a site map.

In the middle of the start page, there should be two blocks of information occupying from 1/2 to 2/3 of the main page with a full name of the SFMS and the website address (left) and brief information about the SFMS (right).

At the bottom of the start page, the following sections should be horizontally centred, presented in a sequential and symmetrical order, in separate rectangular blocks: "Counteraction to Terrorism", "Corruption Prevention", "Public Relations", "National

Risks", "International Cooperation", "State Service", "State Procurement". These headings should be accordingly used in the website structure.

At the bottom of the start page, there should be banners for accessing the SFMS page on Facebook and Twitter.

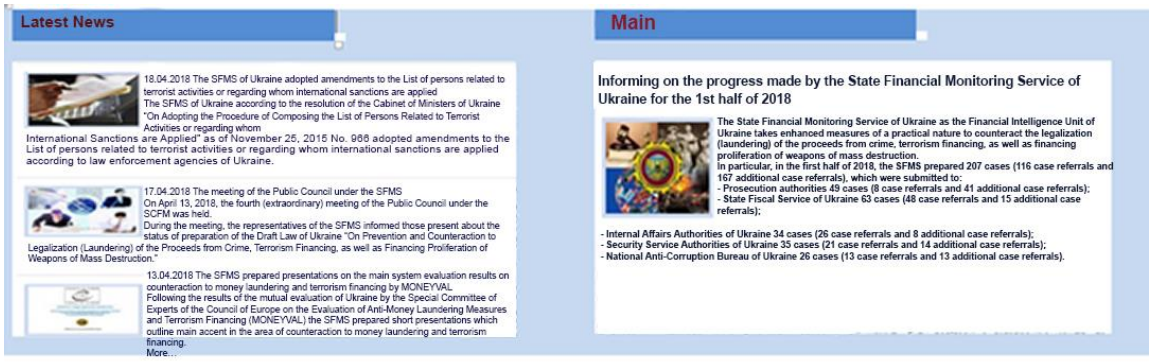
At the footer of each page, there should be an EUACI banner with the following text:

The website is developed with the support of the EU Anti-Corruption Initiative in Ukraine
EUACI is financed by the European Union and Denmark and implemented by Danida

EUACI EUROPEAN UNION ANTI-CORRUPTION INITIATIVE

By navigating the website, the second page should contain 4 rectangular blocks of the same size:

1) The first top left block under the heading "Latest News" should have the SFMS news, with the possibility of forming 6 current news, and further automatic redirection to the archive of relevant news.
2) The second top right "Main" block should contain some information about the main events in the SFMS activities, with the possibility of forming 4 information messages and further automatic redirection to the archive of relevant events.
3) The third bottom left "Analytics" block should contain SFMS analytical information with the possibility of forming 5 analytical information materials placed on the website in the "Activity – Analytics, Typologies" section.
4) The fourth bottom right "Publications" block should have banners of SFMS methodical and practical publications with the possibility of displaying 7 publications placed on the website in the "Methodology – Recommendations" section.



By navigating the website, the third page should contain 2 rectangular blocks of the same size:

1) The first left block under the title “Counteraction to Terrorism Financing” should be divided into 2 blocks: the first should contain news about updates of the SFMS list of terrorists and further redirection to the relevant news archive, the second should contain a current list of terrorists that is posted in the "Counteraction to Terrorism – the List of Terrorists" section.
2) The second right block under the title “International cooperation” should contain banners of 3 international organizations: FATF, MONEYVAL and EGMONT groups, with reference to the corresponding Internet addresses of these international organizations:

http://www.fatf-gafi.org/	https://www.coe.int/en/web/moneyval	https://egmontgroup.org/en
		

At the bottom of the third page there should be a “Partners” section containing a horizontal sequence of banners from the Ukrainian public authorities with whom the SFMS interacts on the state policy implementation in the area of financial monitoring, in the following sequence (from left to right):

- The Ministry of Finance of Ukraine (when the mouse hovers over the banner, "The Ministry of Finance of Ukraine" prompt is displayed; when clicking on the banner there is a redirection to the official website of the Ministry of Finance of Ukraine at http://www.minfin.gov.ua);
- The National Bank of Ukraine (when the mouse hovers over the banner, the prompt "The National Bank of Ukraine" is displayed; when clicking on the banner there is a redirection to the official website of the National Bank of Ukraine at http://www.bank.gov.ua);
- The Prosecutor's General Office of Ukraine (when the mouse hovers over the banner, "The Prosecutor's General Office of Ukraine" prompt is displayed; when clicking on the banner there is a redirection to the official website of the Prosecutor's General Office of Ukraine at http://www.gp.gov.ua);
- The National Anti-Corruption Bureau of Ukraine (when the mouse hovers over the banner, "The National Anti-Corruption Bureau of Ukraine" prompt is displayed, when clicking on the banner there is a redirection to the official website of the National Anti-Corruption Bureau of Ukraine at http://www.nabu.gov.ua);
- The Security Service of Ukraine (when the mouse hovers over the banner, "The Security Service of Ukraine" prompt is displayed; when clicking on the banner there is a redirection to the official website of the Security Service of Ukraine at http://www.ssu.gov.ua);
- The Ministry of Justice of Ukraine (when the mouse hovers over the banner, "The Ministry of Justice of Ukraine" prompt is displayed; when clicking on the banner there is a redirection to the official website of the Ministry of Justice of Ukraine at http://www.minjust.gov.ua);

- The State Fiscal Service of Ukraine (when the mouse hovers over the banner, "The State Fiscal Service of Ukraine" prompt is displayed when clicking on the banner there is a redirection to the official website of the State Fiscal Service of Ukraine at http://www.sfs.gov.ua);
- The National Securities and Stock Market Commission (when the mouse hovers over the banner, "The National Securities and Stock Market Commission" prompt is displayed, when clicking on the banner there is a redirection to the official website of the National Securities and Stock Market Commission at http://www.nssmc.gov.ua);
- The Ministry of Internal Affairs of Ukraine (when the mouse hovers over the banner, "The Ministry of Internal Affairs of Ukraine" prompt is displayed when clicking on the banner there is a redirection to the official website of the Ministry of Internal Affairs of Ukraine at http://www.mvs.gov.ua);
- The National Police of Ukraine (when the mouse hovers over the banner, "The National Police of Ukraine" prompt is displayed, when clicking on the banner there is a redirection to the official website of the National Police of Ukraine at http://www.npu.gov.ua).
- Below the banners of the "Partners" Section in the right half of the website, the banners of the highest authorities of Ukraine (horizontally) are located horizontally (from left to right):
- The President of Ukraine (when the mouse hovers over the banner, "The President of Ukraine" prompt is displayed; when clicking on the banner there is a redirection to the official website of the President of Ukraine at http://www.president.gov.ua);
- The Verkhovna Rada of Ukraine (when the mouse hovers over the banner, "The Verkhovna Rada of Ukraine" prompt is displayed when clicking on the banner there is a redirection to the official website of the Verkhovna Rada of Ukraine at http://www.rada.gov.ua);
- The Government Website (when the mouse hovers over the banner, "The Government Website" prompt is displayed, when clicking on the banner there is a redirection to the official website of the Government Website and at http://www.kmu.gov.ua).

The page background displays the FINTEX style, namely:

- The first start page displays:

- The second start page displays:

- The third start page displays:

Shortcuts.

1. The “Menu” icon contains the following sections and links to them:

- About the Service;
- Documents;
- Activity;
- Coordination;
- Methodology;
- Academy;
- Technology;
- Counteraction to Terrorism;
- Counteraction to Corruption;
- Public Relations;
- International Cooperation;

- National Risks;
- State Service;
- The State Procurement.

The icon 

provides convenient viewing of information on the website for visually impaired users and also provides the possibility of using screen access software that provides data output into audio.

The font size of the text, with the exception of titles, varies up to 200% without the use of auxiliary technologies and loss of information content or the website functionality.

The visual representation of the text has a contrast ratio of at least 5:1.

The website provides convenient navigation using a computer keyboard.

It is not allowed to use time limits for navigating and/or interactive interaction of a user with a website, as well as objects that flash on the screen more than three times per second.

The icon  "The hotline 044-594-16-33" indicates the multichannel phone number, at which primary financial monitoring entities may consult on financial monitoring issues (refer to the heading of section 5.4).

The icon 

(link to the menu heading 7.1) enables switching to an electronic online platform that allows primary financial monitoring entities to submit online information on accounting in the SFMS, on financial transactions subject to financial monitoring, as well as state financial monitoring entities to obtain the information required for the supervision of primary financial monitoring entities.

The icon  allows activating the access to the website in Ukrainian or English.

The icon  enables advanced searching of relevant information on the SFMS website.

The icon 

directs to the page of the State Financial Monitoring Service of Ukraine on WWW.FACEBOOK.COM

The icon  directs to the page of the State Financial Monitoring Service of Ukraine on WWW.TWITTER.COM

The field "Subscribe to our newsfeed" 

allows anyone, by indicating their own e-mail address in the field of the specified service, to receive current news from the SFMS.

The principles of website design should be in line with the functioning of websites of executive authorities.

The Beneficiary chooses and can modify the website at its own discretion:

- the website colour scheme;
- the website content structure (information content).

The organization of information materials on the website has a hierarchical structure, which involves placing data at several levels in the website sections. Within the web pages, structured or separate cross-references are allowed at arbitrary hierarchy levels, depending on a thematic linkage between the data. The control over the relevance of hyperlinks is carried out programmatically and visually.

The main units of the website structure should be chapters, pages and documents (a file different from the HTML page of the structure on which there is a link from the website pages). Pages can include frames, text, tables, forms, and images.

The website enables expanding the structure and volume of materials of each group without significant changes in the overall structure of the group.

The information on the website remains accessible when the website design is disabled, the font size is enlarged, and on the monochrome screen.

Web page appearance: colour, font, information display style (except navigation structure or links) should be universal when the website is viewed from any browser (including mobile browsers) under the design approved by the Beneficiary.

It should be possible to post urgent or breaking news, announcements or advertisements.

The final version of the website design is going to be approved by the Beneficiary by a separate document "Artistic design of the website of the State Financial Monitoring Service of Ukraine".

4.3 Requirements for the Website Structure

The following basic structure should be used for website development:

1. About the SFMS
- 1.1. General information about the SFMS
- 1.2. Leadership
- 1.3. Structure of the SFMS
  - 1.3.1. The leadership of structural units
  - 1.3.2. Main tasks of structural units
  - 1.3.3. Financial resources
  - 1.3.4. General operational rules and internal regulations
  - 1.3.5. Subordinate agencies
- 1.4. Contacts

2. Documents
- 2.1. Laws of Ukraine
- 2.2. Orders
- 2.3. Ordinances and resolutions
- 2.4. Government acts:
  - 2.4.1. Acts of the Ministry of Finance
  - 2.4.2. Acts of the State Financial Monitoring Service
  - 2.4.3. Acts of other state financial monitoring entities
- 2.5. Regulatory activity
  - 2.5.1. Information on the discussion of draft legislation
  - 2.5.2. Draft legislation
  - 2.5.3. Analyses of impact on draft legislation
  - 2.5.4. Reports on tracking the effectiveness of the acts
- 2.6. Risk countries

3. Activity
- 3.1. Strategy

3.2. Performance reports
3.3. Typologies
3.4. Analytics

4. Coordination

4.1. Rada
4.2. Joint acts
4.3. Task forces
4.3.1. Task force – Banking institutions
4.3.2. Task force – Non-banking financial institutions
4.3.3. Task force on sector risk assessment

5. Methodology

5.1. Recommendations
5.2. Standard documents
5.3. Questions and answers
5.3.1. For banking institutions
5.3.2. For non-banking financial institutions
5.3.3. For designated entities
5.4. Hotline

6. Academy

6.1. Financial Monitoring Academy
6.1.1. Training and educational programmes
6.1.2. Guidance materials
6.1.3. Short-term seminars
6.1.4. Contacts

7. Technologies

7.1. FMSA
7.2. Forms for recording and submission of information
7.3. Information interaction technology
7.3.1 For banking institutions
7.3.2. For non-banking financial institutions
7.4. Logical control
7.5. Reference information

8. Counteraction to Terrorism

8.1. List of terrorists
8.2. Documents

9. Counteraction to Corruption

9.1. Report corruption
9.2. Anti-corruption programmes
9.3. Statistical reporting
9.4. Documents

10. Public Relations

10.1. Public Council
10.1.1. Plans and reports of the Public Council
10.1.2. The provision on Public Council
10.1.3. Public Council structure
10.1.4. Public Council meeting minutes and decisions
10.2. Public reception room
10.2.1. Schedule for public reception
10.2.2. Feedback
10.3. Public consultation
10.3.1. Electronic public consultation
10.3.2. Public debate
10.3.3. Public consultation plans and reports

10.3.4. Contacts
10.3.5. Useful links:
- *Regulatory activity (a reference to paragraph 2.5);*
- *Resolution of the Cabinet of Ministers of Ukraine as of 03.11.2010 No. 996 (http://zakon0.rada.gov.ua/laws/show/996-2010-%D0%BF);*
- *Government Website "Civil Society and the Authorities" (http://civic.kmu.gov.ua/consult_mvc_kmu/news/article).*

10.4. Access to public information
10.4.1. Access to public information
10.4.2. Public documents
10.4.3. Reports and common answers
10.4.4. Appeal procedure
10.4.5. Public information accounting system

10.5. Open data:
- *Directory of enterprises, institutions and organizations within the SFMS management, including phone numbers and addresses (entry contains a passport and information file);*
- *Information on the SFMS organizational structure (entry contains a passport and information file);*
- *Report on the use of budget funds, in particular for individual budget programs (entry contains a passport and information file);*
- *Reports, including the addressing of information requests (entry contains a passport and information file);*
- *Annual Procurement Plans of the SFMS (entry contains a passport and information file);*
- *Information on the record system of information stored by the SFMS (entry contains a passport and information file);*
- *Types of information stored by the SFMS (entry contains a passport and a file of information);*
- *Register (list) of open data sets (entry contains a passport and information file);*
- *Administrative data collected (processed) by the SFMS (entry contains a passport and information file);*
- *Legal acts subject to disclosure under the Law of Ukraine "On Access to Public Information" (entry contains a passport and information file);*
- *The financial statements of the State Enterprise "Operation and Property Administration", which belongs to the SFMS management (entry contains a passport and information file).*

10.6. Electronic Appeal

11. International Cooperation

11.1. International activities of the SFMS
11.2. International standards
11.2.1. FATF standards
11.2.2. Council of Europe conventions
11.2.3. UN standards
11.2.4. EU directives
11.2.5. Other standards
11.3. International organizations
11.4. Statements of international organizations
11.5. European integration (EU)
11.6. Euro-Atlantic integration (NATO)

11.7. Memoranda of understanding
11.8. MONEYVAL reports

12. National Risks

12.1. National risk assessment
12.2. National risk documents

13. Civil Service

13.1. Vacancies
13.2. Results of the competitions
13.3. Clarifications
13.4. Lustration of authorities

14. State Procurement

14.1. SFMS Tender Board
14.1.1. Tender Board regulations
14.1.2. Tender Board structure
14.1.3. Contacts
14.2. SFMS procurement plan
14.3. Procurement information
14.3.1. Tender announcements
14.3.2. Protocols of disclosure
14.3.3. Tender reports
14.3.4. Announcements of tender results
14.3.5. Information on appeal examination
14.3.6. Agreements (contracts)

Banners of state authorities:

- Ministry of Finance of Ukraine (http://www.minfin.gov.ua);
- National Bank of Ukraine (http://www.bank.gov.ua);
- Prosecutor General's Office of Ukraine (http://www.gp.gov.ua);
- National Anti-Corruption Bureau of Ukraine (http://www.nabu.gov.ua);
- Security Service of Ukraine (http://www.ssu.gov.ua);
- Ministry of Justice of Ukraine (http://www.minjust.gov.ua);
- State Fiscal Service of Ukraine (http://www.sfs.gov.ua);
- National Securities and Stock Market Commission (http://www.nssmc.gov.ua);
- Ministry of Internal Affairs of Ukraine (http://mvs.gov.ua);
- National Police of Ukraine (http://www.npu.gov.ua).

Banners of state authorities of higher level:

- President of Ukraine (www.president.gov.ua);
- Verkhovna Rada of Ukraine (www.rada.gov.ua);
- Government (https://www.kmu.gov.ua).

4.4 Requirements for the Website for Visually Impaired People

When adapting the SFMS website for people with disabilities, mechanisms for information sharing should be provided based on new technologies that are currently in use.

This subsystem is responsible for displaying the maximum simplified text version of website pages, as well as for increasing the size of the letters on each page of this version and selecting colour pairs for letters and backgrounds.

Website software should provide the most simplified text version of all website pages that provide text output, as well as the possibility of increasing the size of the letters on each page of this version and selecting colour pairs for letters and backgrounds. An example of such solution for the size of the text and letters can be the sample used on

the official website of the Ukrainian Sea Ports Authority (hereinafter referred to as the "USPA"): http://uspa.gov.ua.

There are three ways of moving to a custom page version:

1) A well-visible icon will be placed on each website page, and the following message will be displayed on the website: VERSION FOR VISUALLY IMPAIRED PEOPLE, and when clicked on, there will be a move to the same page, but converted with features that are available now on the USPA site mentioned above;
2) A custom website version should have its own domain blind.fiu.gov.ua, which is a subsidiary website domain. This website version can be found directly without visiting the main website version;
3) When clicking the keyboard shortcuts "Ctrl + B" on the website page, the same page will be opened, but in an adaptive version with features that are currently available on the USPA site mentioned above.

4.5 Mobile Website Version

- The mobile website version is developed as a separate website element and is located at m.fiu.gov.ua.
- The mobile version should provide the information posted on the main website adapted for viewing (use) on mobile devices.

4.6 Requirements for the Number of Users and Operational Staff

- The website should withstand up to 50,000 simultaneous views;
- Support for UTF-8 and WIN1251 encoding should be provided;
- The resolution at which the website will appear at its best: 1920 x 1080; the resolution at which the website will look properly: 1366 x 768, 1280 x 800 and 1024 x 768;
- The website maintenance and administration should be carried out by the staff which has been trained in the website administration; the mode of operation of the staff is one working day.

4.7 Reliability Requirements

The website should maintain the 99.999% operability during a year.

The system must maintain the operability and ensure the recovery of its functions in the event of the following abnormal situations:

- In case of system outage of hardware power supply leads to reboot the OS, the website recovery should occur after rebooting the OS and downloading the necessary website services;
- In case of hardware errors and failures (except for storage medium), the website operability recovery depends on the OS;
- In case of errors related to system software (OS and device drivers), the operability recovery depends on the OS.

5. WEBSITE TECHNICAL REQUIREMENTS

5.1 Common Functionality

The website should have a context-based search information system located in the website database. Search system results are displayed as a list of web page names (with hypertext conversion to each of them) that match the query criteria.

The website should provide the web pages printout. The printable version should contain only the content information of the page provided for printing.

Access, adding and editing dynamic content by administrators and operators.

Administrators and operators may only be appointed among the SFMS staff.

To access the website, the administrator uses a personal account with a relevant password. The administrator has the unrestricted right to publish/edit information or templates in all website sections.

The administrator must be able to create Operators – users with the limited right for the website content.

Persons authorized to add/edit information on the website do this directly from their workplaces. Adding/editing information on the website should be described in the website content documentation.

The CMS shall provide:

- distributed access of administrators and website operators to sections;
- establishment of operators' groups with partial access to separate information sections;
- log keeping of operators' activity, log keeping of changes by operators;
- convenient administration of the rights of groups or individual operators;
- the possibility of the website emergency stop;
- irregular website structure in different languages;
- the possibility of simultaneous operation of operators or administrators.

The CMS should allow administrators and operators to download text, image, video and audio files to the website.

The CMS should have a built-in tool for automatically bringing the content to be placed on the website to a single style (font conversion, font size, spaces, line spacing, etc.).

The CMS should have a high degree of reliability and provide advanced diagnostics and statistics tools, in particular:

- online record keeping of statistics;
- analysing the number of visitors to sections, pages for an arbitrary time period.

The specified parameters can be provided both by a built-in tool and a third-party tool. Detailed requirements will be determined at the technical system design stage. The possibility of obtaining such information should be provided only to SFMS experts.

The Contractor ensures that the website documentation has instructions for deploying the website from backups and distributions.

The CMS should be placed on a separate physical or virtual server and have priority access to the website to avoid a situation when the CMS is not available to internal users due to the excess of the number of simultaneous visitors on the website.

5.2 Graphical User Interface Requirements

All website pages must be executed in a single corporate graphic design style (template).

The service should provide a convenient, user-friendly interface that will ensure:

- quick and easy navigation;
- visual information structuring;
- visual information display;
- sound reproduction of media content;
- compliance with a single corporate style.

The options for designing templates of website pages are approved during the project implementation.

5.3 Linguistic Support Requirements

The website supports interaction with a user in Ukrainian and English languages. The expansion of language components should be provided.

The CMS Language is Ukrainian.

The information and linguistic interaction of the user with the website must be provided by a user-friendly graphical interface.

5.4 Requirements for the Types of Security

It is planned to divide the website into different roles according to the functional purpose and transferring the specified roles to certain physical/virtual servers.

This division will avoid the emergence of "bottlenecks" in the website functioning, which would lead to the failure of the entire website.

Also, the division of servers by roles will allow for flexible scaling of computational capability.

The whole scheme of the website functioning implies the functioning of the server groups for the following services:

- Website Management System;
- Customer Service;
- Search;
- DBMS.

5.5 Requirements for Users

The website should ensure the access rights differentiation to certain information resources and subsystems based on a role-based access model of users to the SFMS website.

The following user roles are defined for the website operation:

- Security Administrator;
- Server Hardware Administrator;
- Website Administrator;
- Website Operator;
- Financial Monitoring Entities;
- Anonymous Users.

The main responsibilities of the **Security Administrator** are:

- organization and control of the high-quality implementation of organizational and technical measures for information protection on the website;
- management of ISFM access attributes used to access website resources;
- management of website event audit logs;
- configuration and monitoring the TCB security parameters;
- monitoring of the TCB functioning;
- organization and control of backup and recovery of critical information stored in ISFM.

The main responsibilities of the **Server Hardware Administrator** are:

- configuration, performance monitoring and upgrade of the website software and hardware means;
- development and maintenance of virtual machines in the website;
- installation, uninstallation, upgrade, configuration and monitoring of the system and custom software website operability;
- installation, uninstallation, upgrade and initial configuration of the functional website software;
- organization and implementation of website backup and recovery under the relevant instructions.

The main responsibilities of the **Website Administrator** are:

- installation, configuration and monitoring of website application software;
- maintenance of website administrative accounts;
- management of user access rights to website functions;
- editing the content of the public website;
- monitoring the operation of websites, analysing web server software event logs;
- informational support of users in matters concerning the public website and FMSA website.

The main responsibilities of the **Website Operator** are the website content management.

The main functions of users with the role of **Financial Monitoring Entity** are the interaction and exchange of information with ISFM within the functions provided by the FMSA service.

The main functions of users with the role of **Anonymous User** are the familiarization with the information posted on the public ISFM website.

All rights of access and authentication rules are defined within the existing access rights differentiation system between users of the SFMS website system.

5.6 Technical Requirements for Website Implementation

The website will be integrated into the ISFM and will use the software and hardware means now involved in the website maintenance.

The website should be built on the client-server architecture with the ability for website users to work through the web interface.

The website software and hardware should provide for the centralized data placement at the Beneficiary's location.

The service should operate based on a free and open-source software, preferably the CentOS platform of version not lower than 7 with pre-installed PostgreSQL database server and website software.

The website as a software product is provided as program modules for a website.

Website Management System Service

It applies exclusively by operation staff to fill the website information structure and content. Also, this service is a source of information on the website, from which the distribution of the added information to other servers takes place.

Customer Service (Front-End Server)

It is designed to execute the source code of the website and serving user queries. The website source code is downloaded to the server automatically from the source code system (Git, Mercurial). The main purpose of the server is to execute user requests as part of generating website pages.

Search Service

It is designed to process search queries for an information component of a website (processes "site search" queries and processes search queries and queries from a system of a nationwide bank of vacancies and CVs).

The inaccessibility of this server should not affect the overall website availability.

Database Management System (DBMS)

It is designed to store structured data of the website.

5.7 Software Requirements

The website software should include a general (or system) and custom software.

Website servers should run on a free and open-source software, preferably the CentOS operating system of version not lower than 7.

As the website DBMS, it is necessary to use a free and open-source software, preferably PostgreSQL or any other by an agreement with the Beneficiary.

The client part of the website should be supported by modern, commonly used browsers (including mobile ones).

Programming languages and technologies that should be used to develop a website and management system: PHP, PostgreSQL, a modern JavaScript-based Framework for computing and client-side routing functions, a modern PHP Framework that implements the MVC paradigm, with the ability to use ActiveRecord, caching data, the possibility of internationalization and the use of a modern PHP dependency manager. The development of web page templates should be done using technologies such as HTML 5, CSS 3, JavaScript.

The website software should meet the requirements specified in section 4.6.

Website pages should be displayed correctly in the following browsers:

- Internet Explorer (version 10.0 and higher);
- Opera (version 49 and higher);
- Safari (version 7.0 and higher);
- Mozilla Firefox (version 35 and higher);
- Google Chrome (version 49 and higher);
- etc.

5.8 Additional Services and Features

A block of links to the most relevant (popular) sections of the website should be created based on the statistics of the number of visits to web pages during the last month.

When developing information pages, it is necessary to consider the possibility of adding links to social networks (for example, twitter.com, etc.).

6. WEBSITE INFORMATION PROTECTION REQUIREMENTS

6.1 General Requirements for Website Information Protection

Clear information protection placed on the website is carried out under the applicable law.

The information protection subsystem should provide:

- user's access rights differentiation to protected resources of the website at the level of tasks and data stores;
- user identification and authentication;
- verification of user authority and granting the right to perform certain actions with protected resources (reading, modifying, destroying, information input, etc.);
- recording events related to access to the website resources, the results of user identification and authentication, the changes of the user authority, the results of information protection integrity verification;
- blocking unauthorized actions on the website resources and automatically informing the designated person of such actions.

Registration data (audit reports) must be protected against unauthorized modification and destruction by users, including those having security administrator authority.

The website security information subsystem should include automated registration data analysis tools.

The website security information subsystem should be in conformity with the legislation in the TPI field.

Passwords should be used in the website security information subsystem (in the case of a password set, its characters are not displayed on the screen or replaced by one-character type; the number of characters does not match the password length).

The information security subsystem should automatically block user sessions and applications upon completion of the specified time of user inactivity.

The management of information protection and means of control are carried out by an authorized person – a Security Administrator.

The proper website functioning is ensured by adhering to the software integrity used to process the information on the website as well as antivirus protection implementation of such information.

To provide enhanced security, users' access to the website should be done using the modern cryptographic protocols (for example, HTTPS).

6.2 Requirements for Ensuring Integrity

Website software should:

- ensure the integrity of the website software modules;
- ensure data integrity during processing;
- include the possibility of ensuring data integrity during transmitting through open communication channels by cryptographic means not included in the website.

6.3 Requirements for Ensuring the Recording of Events

Website software should ensure the recording of the following security events:

- actions of all users in the administrative part;
- user failed authentication attempts;
- account operations;
- attempts for unauthorized access to the website;
- attempts for information copying, downloading/unloading.

The list of other security events recorded on the website software is agreed at the technical project stage.

6.4 Requirements for Information Access Security

During website development it is necessary to consider the requirements for state information Internet resources specified in the Order of The State Service of Special Communications and Information Protection of Ukraine as of 02.04.2003, No. 33 "On the Enactment of the Regulatory Document "ND TZI 2.5-010-03 Requirements for Information Protection of the WEB-page from Unauthorized Access."

The protection of information contained on the website from unauthorized access should be ensured by managing user access rights and software modules to the website data.

The website should ensure a positive user experience and provide modern cybersecurity protection mechanisms.

It shall be possible to block advertisements and execute various third-party scripts not foreseen on the website itself, but arising from malware infection of the user's personal computer, namely:

1) preventing the emergence of pop-ups by a ransomware on a website, as a result of infecting a user's personal computer;
2) protection against malvertising attacks by the latest algorithmic mechanisms for their detecting and neutralizing;
3) protection against "Outbrain" techniques and banner injections of malicious code into client-side browser pages;
4) protection against "ZeroDay" attacks by advanced technologies and methods for preventing injections of malicious code on the client side;
5) use of adaptive and behavioural algorithms for monitoring web traffic and real-time risk management.

When using this system, there should not be excessive load on the server part to ensure the high-performance rate of the website.

6.5 Requirements for Information Storage in Case of Accidents

There should be a daily automated procedure for backing up databases and saving user software configuration settings. The frequency of backing up or the procedure for their determination should be set out in the operational documentation.

It should be possible to recover the website operability by backups after a partial or complete refusal, by means which only the administrator can use. The description of the procedure itself should be in the relevant documentation.

Backups should be stored on independent physical media. If possible, they must be stored on the technical site, separate from the main one.

6.6 Staff Training

The Contractor shall provide the website and CMS training for the communication expert of SFMS.

7. STANDARDIZATION AND UNIFICATION REQUIREMENTS

The website implementation should be carried out by commercial hardware and computing network hardware.

During implementation, it is necessary to be guided by:

- State Committee of Ukraine for Standardization, Metrology and Certification (DSTU);
- regulatory and guidance documents of the legislative and executive authorities;
- relevant departmental regulatory and guidance documents.

8. LICENSE REQUIREMENTS AND OWNERSHIP

The website should only operate on a free and open-source or licensed software.

All exclusive intellectual property rights to:

- software developed for the website,
- the results of works and/or services performed and/or rendered to the Customer that are the intellectual property,

belong to the Customer and will later be transferred to the Beneficiary.

The website should be implemented as an open system that enables its development and modification by expanding its functionality, connecting new information resources and expanding the range of users.

9. ORGANIZATIONAL SUPPORT REQUIREMENTS

To ensure the stable website operation, it is necessary to appoint administrators and the designated person when it is put into service.

The training of CMS operators and administrators should be carried out to ensure the website implementation by the Contractor.

10. PROCEDURE FOR WEBSITE MONITORING AND ACCEPTANCE

Upon completion of the website development, a stand-alone test should be conducted.

Upon completion of stand-alone tests, comprehensive preliminary testing of the website should be conducted.

Upon completion of the comprehensive preliminary testing, the website operation testing should be conducted.

According to the positive results of website check tests, it is put into the production run.

11. DOCUMENTS PROVIDED AFTER COMPLETING THE RELEVANT PHASES AND STAGES OF WORKS

The Contractor agrees and, according to the work results, provides documents on the following list:

- Technical Design Specification;
- General System Description (Front-end and detailed design, Explanatory Note);
- General description of the compliance of built-in website protection mechanisms with the security profile requirements (The IIPS front-end and detailed design, The IIPS explanatory note);
- Specification;
- User Manual;
- Administrator Manual;
- Web Security Administrator Manual;
- Website Testing Program and Techniques;
- Preliminary Protocols;
- Operational Acceptance Certificate;
- Testing Protocols of Site Vulnerabilities;
- Production Acceptance Certificate;
- The list of documents can be specified at the website design stage.

All technical and user documentation should be prepared on paper and optical CDs (in Microsoft Word and Adobe PDF format).

12. PROJECT TIMELINE

The intended commencement date is 22 October 2018. The website shall be made operational by 15 February 2019.

The following phases are foreseen:

1. **Consultation and inception**. In this first phase, the Customer is expected to liaise with the Contractor, clarify the remaining questions and provide expert recommendations on the structure design of the webpage.
2. **Website design and development**. Based on the previous phase, the website is going to be established. The Contractor is expected to present the website design to the Customer and incorporate the feedbacks during this development phase.

3. **Testing phase**. The website is going to be tested for a certain period of time, the errors are going to be reported in the "Test Report" document.
4. **Finalization and launching of the website**. This is going to include fixing of any bugs, errors or unexpected behaviour reported in the document "Test Report" by the SFMS, deployment to the production environment.

13. BIDDING DETAILS

The bidder must submit the following information to be considered:

1. A brief profile (maximum two pages) of the company.
2. Provide the total number of bidder's employees and the number of employees in user experience and web design.
3. The CVs (no more than three pages for each person) of the key team members who will be involved in the project. List the names, project titles, key duties of this assignment and amount of time dedicated to this project.
4. A list of assignments, similar to this project, executed in the last five years (must include website addresses).
5. Provide a detailed description of the methodology, scope of work and timeline of the project as well as key assumptions.
6. Provide the budget for the services in euro, inclusive of all taxes or other such charges.

14. HOW TO APPLY

Deadline for submitting the proposals is **12 October 2018, 18:00 Kyiv time.**

The proposals shall be submitted within the above deadline to Barbara James, barjam@ukraine-aci.com, cc: Oleh Pasko, olepas@ukraine-aci.com.

Bidding language: **English**.

Any clarification questions for the request for bid should be addressed to olepas@ukraine-aci.com, cc: barjam@ukraine-aci.com, not later than 9 October 2018, 18:00 Kyiv time.

15. EVALUATION CRITERIA

Bids will be evaluated in accordance with criteria provided below:

#	Criteria	Weight
1	Portfolio of projects successfully completed on website's design and development, quality and relevance of past work	40%
2	Key delivery team members: relevant experience, skills and competencies	15%
3	Proposed methodology and detailed timelines	15%
4	Proposed budget	30%

European Neighbourhood Department (EUN)
Ministry of Foreign Affairs of Denmark
Copenhagen
4 October 2018