

Terms of Reference

Regarding

**Request for bid for conducting of
Information Technology audit of National Agency of Ukraine for Finding, Tracing and Management of Assets Derived from Corruption and other Crimes**

# Abbreviations

|  |  |
| --- | --- |
| ARMA | National Agency of Ukraine for Finding, Tracing and Management of Assets Derived from Corruption and other Crimes |
| ARMA ITS | ARMA’s information and telecommunication system (including information and telecommunication systems of ARMA’s interregional territorial units) |
| AE | analysis element |
| DSTU | State Standard of Ukraine |
| EU | European Union |
| EUACI | European Union Anti-Corruption Initiative |
| GOST | Set of technical standards maintained by the Euro-Asian Council for Standardisation, Metrology and Certification (EASC) |
| KSZI | comprehensive information protection system, a set of organisational, engineering and technical measures aimed at ensuring the protection of information from disclosure, leakage, and unauthorised access |
| IT | Information Technology |
| ICT | Information and Communication Technology |
| ITS | information and telecommunication system — an organizational and technical system that implements information technology and combines a computer system, the physical environment of its location and operation, personnel (user environment), and processed information, including the technology for processing thereof |
| IS | Information Security |
| MFA | Ministry of Foreign Affairs of Denmark |
| ND TZI | regulatory instrument of technical information protection system |
| OS | Operating System |
| SSSCIP | Administration of the State Service of Special Communications and Information Protection of Ukraine |
| TOR | Terms of Reference |
| TCB | Trusted Computing Base |
| assessment | determining the degree of compliance of the inspected item’s features with the set criteria and requirements |

# Background and context

**General overview**

EUACI is the comprehensive EU anti-corruption program in Ukraine financed by the EU and Denmark and implemented by the MFA of Denmark.

The overall objective of the EU and Danish funding for anti-corruption efforts in Ukraine is to improve the implementation of anti-corruption policy in Ukraine, thereby ultimately contributing to a reduction in corruption. The EUACI is aimed at strengthening the capacity of the newly created anti-corruption institutions and enhancing external oversight over the reform process by the Verkhovna Rada, civil society and the media.

The work of the EUACI is streamlined through its 3 components: (1) strengthening the operational and policy-making capacities of state institutions dealing with the prevention and fight against corruption; (2) enhancing the capacity of local self-government, civil society, media, and business to contribute to the fight against corruption; and (3) increasing culture of integrity issues in Ukraine through the engagement of the business sector, the civil society and the media.

Within component 1 the EUACI is working with the National Anticorruption Bureau of Ukraine (NABU), National Agency for Corruption Prevention (NACP), Assets Recovery and Management Agency (ARMA), Special Anticorruption Prosecutor’s Office (SAPO), State Financial Monitoring Service (SFMS), High Anti-Corruption Court of Ukraine (HACC), Parliament’s Committee on Anti-Corruption Policy (CAP).

**Beneficiary**

Subject to the continuation of the EUACI international technical assistance project for the period 2020-2024, ARMA and EUACI agreed on the work plan for cooperation during the implementation of the EUACI Phase II, which, inter alia, provides assistance to strengthen ARMA's IT capacity.

According to the work plan, it is envisaged that in 2021-2022 ARMA will conduct an IT audit, the conclusions and recommendations of which should form the basis of ARMA's IT Strategy, as well as become the basis for ensuring the safe operation and sustainable development of ARMA in the field of IT.

ARMA requests assistance to implement this activity to support its further needs for IT capacity building.

In the course of the IT audit by ARMA’s request, it is planned to conduct an examination of:

* the computer system (network, server, and operating architecture, security infrastructure);
* the physical environment (physical infrastructure and organizational environment);
* the user environment;
* the information environment (processed information and technology of its processing).

During the first stage of implementation of this activity (August-October 2021) “Requirements for inspecting the components of the information and telecommunication system and its operating environments” were developed and approved by ARMA.

This TOR is based on the abovementioned document and contains the main requirements, technical and qualitative characteristics, the scope of work on the audit of information technology, namely information and telecommunications system (ITS) and its information environments of ARMA (hereinafter – ARMA ITS).

Owner of ARMA ITS: National Agency of Ukraine for Finding, Tracing and Management of Assets Derived from Corruption and Other Crimes.

The examination shall be restricted by the physical boundaries of ARMA’s premises where the ARMA ITS components are located (including ITSs of ARMA’s regional territorial units).

**Contracting authority**

The contracting authority is the European Union Anti-Corruption Initiative in Ukraine, supported by the EU and Denmark and implemented by the Ministry of Foreign Affairs of Denmark, hereinafter referred to as the Customer.

**Purpose**

The purpose of conducting the examination of ARMA ITS is the assessment of the existing IT resources’ conformity to the requirements of current business processes, identification of shortcomings, and drafting of recommendations for effective planning of the development of ARMA’s IT resources (development of an IT strategy for the ARMA capacity building).

Inspection of ARMA ITS should be conducted to prepare data for:

* recommendations for optimal development (upgrade) of ARMA ITS’s network, server and operating architecture, and of information processing technology in ARMA ITS;
* unification of the ARMA ITS components’ software and hardware;
* determination of the need to create (upgrade) KSZI in ARMA ITS and to design general requirements for the KSZI in the form of a description of each operating environment with identification of its components that may, either directly or indirectly, affect IS;
* identification of interference between components of various environments, documenting the inspection findings;
* determination of the feasibility and expediency of developing recommendations for a standard approach to the KSZI deployment in ARMA ITS (including KSZI in ITSs of ARMA’s interregional territorial units).

Deliverables from the ARMA ITS examination should be suitable for:

* development of ARMA IT strategy;
* designing the ARMA ITS development concept;
* designing the development (upgrade) plan for the ARMA information infrastructure;
* ensuring safe operation and sustainable development of the ARMA information infrastructure;
* planning and conducting penetration testing (pen test) of ARMA ITS;
* planning of advanced training for employees from the ARMA units responsible for the functioning of ARMA ITS.

# Objective

The overall objective of this assignment is to conduct an examination of ARMA ITS, taking into account the above purpose and the fulfilment of the requirements described in this TOR.

In order to ensure the highest reliability and completeness of findings when organizing and conducting the ARMA ITS examination, the following basic principles for the conduct thereof shall be observed:

* independence, responsibility, and competence of the experts engaged in the conduct of the examination;
* completeness of the assessment;
* assessment based on available certificates, etc., for the ARMA ITS components.

# Scope of Work

Examination of ARMA ITS (including ITSs of ARMA’s field offices) shall include, but not be limited to the following set of activities:

* 1. Preliminary review of ARMA ITS.
	2. Planning the ARMA ITS inspection.
	3. Examination of ARMA ITS and analysing the findings:

**3.1.** Examination of the components of ARMA ITS:

* network architecture;
* server architecture;
* operating architecture;
* physical infrastructure;
* security infrastructure;

**3.2.** Examination of the operating environments of the ARMA ITS components:

* information environment;
* user environment;
* organizational environment.
1. Documenting and approving the findings of the ARMA ITS examination.

A detailed description of requirements for examination is given in [Appendix 1](#_Appendix_1_Website) of this TOR.

# Deliverables

The following deliverables shall be provided by a Contractor:

**1. Deliverables of the preliminary review of ARMA ITS**

Deliverables of the preliminary review of ARMA ITS shall include, but not be limited to the working materials in which the experts who have analysed the relevant materials and reviewed ARMA ITS should state their opinion of:

* the degree of ARMA ITS’s conformity to the information provided;
* the completeness of the design, operating, regulatory and administrative documentation provided;
* justify the decision on the feasibility of carrying out further inspection work or on termination thereof;
* clarify proposals for the plan and sequence of carrying out any further work.

Furthermore, recommendations may be given on the need to refine the submitted documents, develop additional documents or provide additional materials that should be used at subsequent inspection stages.

**2. Deliverables from planning the ARMA ITS examination**

Deliverables from planning the ARMA ITS examination shall include but not be limited to the ARMA ITS Inspection Program developed and coordinated with the ARMA.

When documenting the ARMA ITS Examination Program, experts should observe the requirements of GOST 19.301-79, DSTU 2853-94, other applicable standards and regulatory instruments in the field of IT and information protection, which concern the preparation and conduct of the examination.

**3. Deliverables from the ARMA ITS examination and analysing the findings**

Outcomes from the examination of ARMA ITS and analysing the findings shall include the performance of the full scope of the examination work stipulated by the approved ARMA ITS Examination Program by taking certain actions and conducting checks.

Deliverables from the ARMA ITS examination shall be finalized as the Examination Findings Report for the ARMA ITS components and their operating environments.

**4. Deliverables from documenting and approving the ARMA ITS examination findings**

Deliverables from documenting and approving the ARMA ITS examination findings shall include the compiled and approved Examination Findings Report for the ARMA ITS components and its operating environments.

Examination Findings Report for the ARMA ITS components and its operating environments, should include, but not be limited to the following parts:

1. findings of the ITS computer system analysis:
* network infrastructure;
* server infrastructure;
* operating infrastructure;
* security infrastructure;
1. findings of the ITS operating environment analysis:
* information environment (including processing technology);
* physical environment;
* user environment (personnel);
1. findings of the ITS organizational structure analysis:
* rules for the ITS operation;
* the structure and role composition of the ITS functional user teams;
1. findings of the analysis of information security provisions;
2. assessment of ITS assets and suggestions for optimal development (upgrade) of ARMA ITS’s network, server, and operating architecture, and of information processing technology in ARMA ITS;
3. suggestions for the unification of the ARMA ITS components’ software and hardware;
4. recommendations for the development (upgrade) of the KSZI in ARMA ITS, in the form of a description of each ARMA ITS’s operating environment, listing the components of various environments, which may, either directly or indirectly, affect IS;
5. opinions of the findings from the examination of the ARMA ITS components and its operating environments.

The Examination Findings Report for the ARMA ITS components and its operating environments shall be signed by the inspecting experts and duly approved by ARMA.

The Examination Findings Report for the ARMA ITS components and their operating environments shall be finalized and submitted according to the provisions of DSTU 3396.1-96, ND TZI 3.7003-05.

All documentation must be prepared in paper and electronic forms in Microsoft Word and/or Adobe PDF format.

# Timing

The assignment shall start following a notification issued by the contracting authority, but not earlier than the date of signing the contract between the EUACI and the Contractor.

The intended commencement date of the conducting of the examination of ARMA ITS is 20 December 2021. The estimated time for the examination is up to 6 months starting from signing the contract.

# Methodology

It is envisaged that the assignment will be implemented by a team of experts familiar with the context and experienced with similar assignments.

By conducting the examination of ARMA ITS, a contractor shall work in close cooperation with the appropriate ARMA’s staff and shall perform on-site visits of the relevant services, desk review and consultations. The experts shall make use of all provided legislation, regulations, studies, reports and other relevant documents like statistics, background materials provided by the ARMA. Moreover, ARMA shall provide in due time any additional data, reports, analysis, statistics, studies, etc. identified as relevant by the experts during the lifetime of the implementation of this assignment.

By putting forward a team of experts, the Contractor shall ensure that the task will be developed with as much straightforwardness as possible, the proposed approach and the methodology shall be fine-tuned and a detailed work plan shall be elaborated.

# Estimated budget

The maximum budget for this assignment all included may not exceed DKK 223 067 (approximately EUR 30 000), including all expenses for travelling to ARMA’s regional territorial units.

# Reporting and management

The performance of the Contractor will be judged upon reaching the purpose of this assignment as well as obtaining its results, as indicated in the section “Scope of work” and “Deliverables” herein respectively.

By signing the contract, the Contractor agrees to hold in trust and confidence any information or documents, disclosed to the Contractor or discovered by the Contractors or prepared by the Contractors in the course of or as a result of the implementation of the contract, and agrees that it shall be used only for the task implementation and shall not be disclosed to any third party.

In the period until acceptance, the EUACI, Contractor, and ARMA will hold working meetings to exchange information and seek to clarify any questions of whatsoever nature. The purpose of the meetings is to ensure follow-up on any activities between the meetings, to maintain a common overview of the current stage of the assignment at a detailed level, and to ensure the day-to-day progress.

# Background documents

The implementation of the assignment shall meet provisions of laws and regulations, such as:

* The Law of Ukraine on Information.
* The Law of Ukraine on Access to Public Information.
* The Law of Ukraine on Information Protection within Information and Telecommunication Systems.
* Rules for ensuring the protection of information in information, telecommunication, information, and telecommunication systems, as approved by the Resolution No. 373 of the Cabinet of Ministers of Ukraine dated 03/29/06
* DSTU 2226-93. Automated systems. Definitions.
* DSTU 3396.1-96. Information Protection. Technical Information Protection. Order of Carrying out the Works.
* DSTU 3396.2-97. Information Protection. Technical Information Protection. Definitions.
* DSTU ISO/IEC TR 13335-3:2003 Information Technologies. Guidelines for the Management of IT Security. Part 3. Techniques for the Management of IT Security.
* ND TZI 1.1-002-99 General provisions for protecting information in computer systems against unauthorized access
* ND TZI 1.1-003-99 Terminology in the field of protecting information in computer systems against unauthorized access
* ND TZI 1.1-005-07 Information protection at information activity facilities. Setting up a technical information protection complex. Key Provisions.
* ND TZI 3.7-003-2005. Procedure for setting up a comprehensive information security system in the information and telecommunication system.

# How to apply

The deadline for submitting the proposals is **14 December 2021, 17:00 Kyiv time**.

The bidder must submit the following information to be considered:

1. Brief company profile (maximum 2 pages).
2. The CVs of experts (no more than 3 pages for each expert).
3. List of projects with a short description (up to 3 projects), similar to this one, in which the experts involved in this project took part in the last 3 years.
4. Brief description of the methodology (no more than 4 pages) of the proposed consultation.
5. Financial proposal with a budget for services in Euros (including all expenses for travelling to ARMA’s regional territorial units).
6. Copies of certificates and permits as specified in [Appendix 2](#_Appendix_2._) and [Appendix 3](#_Appendix_3._The) to this TOR.

The applicant should meet the qualification requirements as described in [Appendix 2](#_Appendix_2._) of this TOR.

The proposals shall include the aforementioned information and should be submitted within the above deadline to: serkon@um.dk, indicating the subject line “**ARMA IT audit**”,

Bidding language: English.

Any clarification questions for the bid request should be addressed to: serkon@um.dk no later than **6 December 2021, 17:00 Kyiv time.**

# Appendix 1 Requirements for examination of ARMA ITS

1. **Preliminary review of ARMA ITS**

The purpose of the preliminary review of ARMA ITS is to make a decision on the feasibility of conducting the ARMA ITS examination, determine the scope and schedule of subsequent activities.

The following steps should be taken during the preliminary review of ARMA ITS:

* preliminary analysis of the input data on ARMA ITS, as provided by ARMA, in order to obtain and process initial information about the key information protection requirements imposed by applicable regulatory instruments and to be met by ARMA ITS, as well as the key ARMA ITS features to be validated during the examination;
* review of ARMA ITS in its actual operating environment to determine the degree of its readiness for examination activities;
* preliminary analysis of the design, operating, regulatory and administrative documentation provided by ARMA for conformity of the structure thereof to the requirements of applicable regulatory instruments;
* documenting the findings and deciding on proceeding with or terminating any subsequent activity stages.

Following the analysis of these materials, a preliminary opinion is developed of:

* the architecture of ARMA ITS;
* the class and subclass of ARMA ITS as an automated system in accordance with the provisions of ND TZI 2.5-005-99;
* the information resources processed by ARMA ITS, which are subject to protection under applicable laws and regulations, and their processing technology;
* the features of information in accordance with the legal regime and access regime (publicly available information; publicly available information included into state information resources; confidential information; privileged information and confidential information held by information owners that are defined by Article 13.1 of the Law of Ukraine on Access to Public Information; information that constitutes a state secret, is contained in certain information resources and requires protection in accordance with the provisions of applicable laws and regulations), as established by the Law of Ukraine on Information and by other legislative acts;
* the provisions, which must be met by the KSZI, of applicable regulatory instruments as to the protection of certain properties (confidentiality, integrity, availability) of information processed in ARMA ITS;
* the ARMA ITS’s functional structure and its main features that must be validated during the examination (a list of organizational, physical, and other measures of protection, etc.);
* the location, category, and other general features of the ITS, within which ARMA ITS has been created and operates.

When reviewing ARMA ITS in the actual operating conditions of the ITS, efforts of inspecting experts should be primarily focused on collecting the evidence that attests to the fact that ARMA ITS exists in the same structure and with the same features that were identified during the previous review of input data about ARMA ITS.

When conducting a preliminary analysis of the delivered ARMA ITS documentation for compliance with applicable regulatory instruments, the structure of the design, operating, regulatory and administrative documentation delivered by ARMA should be checked, with regard to the findings of the preliminary analysis of the input data about ARMA ITS, for compliance with applicable regulatory instruments.

1. **Planning the ARMA ITS examination**

The purpose of planning the ARMA ITS examination is to develop and coordinate the ARMA ITS Examination Program with ARMA.

Any materials collected, analysed, and, where necessary, refined by ARMA should be used as input data.

The developed ARMA ITS Examination Program should provide, but not be limited to a description of:

* the precise requirements and the sequence in which ARMA ITS should be checked to validate or negate its compliance with the provisions of the TORs for the ITS design or with those of the TIP system’s applicable regulatory instruments;
* the purpose of and the grounds for the examination;
* the sequence and timing of the examination work;
* the composition of the expert team.

The ARMA ITS Examination Program should stipulate, but not be limited to the following:

* analysis of documentation developed at the pre-design stage;
* analysis of the TORs for the ITS design;
* analysis of the ITS design documentation and materials containing the findings of the state expert examination (certification) of individual components of ARMA ITS’s TCB;
* analysis of operating documentation for components (constituent parts) of ARMA ITS’s TCB;
* analysis of ARMA ITS’s regulatory and administrative documentation;
* analysis of the documentation on tests performed on ARMA ITS;
* analysis of ARMA ITS’s managerial and regulatory documentation;
* checking the procedure for using the information protection facilities integrated into the TCB;
* checking the implementation of organizational, physical, and other non-technical measures of protection deployed within ARMA ITS;
* checking the degree of training of ARMA ITS’s personnel and users.
1. **Inspection of ARMA ITS and analysis of the findings**

The purpose of inspecting ARMA ITS and analysing the findings is to perform the full scope of examination work stipulated by the approved ARMA ITS Examination Program by taking certain actions and conducting checks followed by the analysis of the findings.

In the course of the examination of ARMA ITS (incl. ITSs of ARMA’s regional territorial units), it should be regarded as an organizational and technical system that combines:

* computer system (network, server, and operating architectures, security infrastructure);
* information environment (processed information and its processing technology);
* physical environment (physical infrastructure and organizational environment);
* user environment (personnel).
	1. ***The examination of the ITS computer system shall analyse and describe, but not be limited to:***
* the overall structural arrangement and composition (list and composition of equipment, technical and software tools, their interconnections;
* configuration, architecture and topology features;
* software, hardware/software information protection facilities, mutual siting of facilities, etc.);
* types and features of communication channels;
* specifics of inter-component interaction and influence;
* potential restrictions on the use of certain facilities, etc.

Those computer system components must be identified that contain or lack information protection facilities and mechanisms, along with the potential of such facilities and mechanisms to ensure the protection of Information, their respective properties, and features, including those set by default, etc.

Any presented findings of the ARMA ITS computer system examination should provide comprehensive information about the potential of ARMA ITS’s computer system both in terms of supporting the functioning of ARMA ITS’s system-wide and application software, and supporting the functioning of the protection facilities that can be implemented and deployed in the process of creating (upgrading) the KSZI in ARMA ITS.

Based on the findings of the analysis, a general idea is developed about the availability of potential opportunities for ensuring information protection, identifying those ARMA ITS components that call for stricter information protection requirements, and implementation of additional security measures.

***3.2. When inspecting the information environment***, all the information processed and stored in ARMA ITS (data and software) shall be subject to analysis. During the analysis, the information shall be categorized according to the access mode, legal regime, and the defined and described types of its presentation in ARMA ITS.

Each kind of information and the type of object containing it shall correlate with the information security properties (confidentiality, integrity, availability) that they must meet.

Following the analysis of information processing technology, the specifics of the electronic document workflow are identified; information flows and their transmission media, flow sources and their destinations, information flow management principles, and methods are defined and described; block diagrams for the flows are developed. The types of information media and the procedure for using thereof in the operation of ARMA ITS must be recorded.

For each structural element in the information flow diagram, the composition of information objects, the access mode to them, and the potential impact from the user environment, the physical environment in terms of preservation of information properties is recorded.

***3.3. When inspecting the physical environment (physical infrastructure and organizational environment)***, the location of ARMA ITS’s information processing facilities at information activity objects, utilities, sustainment and communication systems, and the mode of operation of these objects are analysed.

The examination should be conducted in compliance with DSTU 3396.1.

The following features of ARMA ITS’s physical infrastructure shall be analysed:

* location of the ITS components (master plan, situation plan);
* availability of security and access control;
* availability of categorized premises where the ITS components are to be sited;
* access mode to the ITS physical environment components;
* impact from environmental factors;
* presence of utilities, sustainment, and communication system components that extend beyond the controlled area;
* availability and specifications of grounding systems;
* storage conditions for magnetic, magneto-optical, paper, and other information media;
* availability of design and operating documentation for physical environment components.

When inspecting ARMA ITS’s organizational environment, the analysis should be performed of ARMA ITS’s organizational structure, the structure and role composition of the ARMA ITS administration and operation units, rules for ARMA ITS’s users (personnel).

***3.4. When inspecting the user environment (personnel), the following shall be analyzed:***

* functional structure and number of users, their functional responsibilities, and qualification levels;
* user powers to access information processed by ARMA ITS, to have access to ARMA ITS and individual components thereof;
* capability levels of various user categories, as provided (or may be available) to them through ARMA ITS’s facilities;
* user rights to manage ARMA ITS;
* observability of ARMA ITS.

***3.5. Conduct the examination under the developed ARMA ITS Examination Program*** (concerning the specifics of ARMA ITS) shall involve, but not be limited to the following:

* analysis of documentation developed at the ARMA ITS pre-design stage;
* analysis of the Terms of Reference for the ARMA ITS design;
* analysis of the ITS design documentation and materials containing the findings of the state expert examination (certification) of individual components (constituent parts) of ARMA ITS’s TCB;
* analysis of operating documentation for components (constituent parts) of ARMA ITS’s TCB;
* analysis of ARMA ITS’s regulatory and administrative documentation;
* analysis of the documentation on tests performed on ARMA ITS;
* analysis of ARMA ITS’s managerial and regulatory documentation;
* checking the procedure for using the information protection facilities included in the TCB;
* checking the implementation of organizational, physical, and other non-technical measures of protection deployed within ARMA ITS;
* checking the degree of training of ARMA ITS’s personnel and users;
* analysis of the findings of the ARMA ITS examination.
1. **Documenting and approving the ARMA ITS examination findings**

The purpose of documenting and approving the ARMA ITS examination findings is to perform the full scope of work to record the experts’ opinions of the outcomes of execution of the ARMA ITS Examination Program.

The opinions formulated by the experts, following the examination performed under the ARMA ITS Examination Program, shall be recorded in the Examination Findings Report for the ARMA ITS components and its operating environments. This report should record both the experts’ opinions and (either directly or by reference to the analysed materials and documents) the arguments based on which the respective opinions were formed.

# Appendix 2. Qualification requirements for the contractor

The Contractor for the ARMA ITS examination should have:

* 8+ years of proven experience in the field of information protection (information security);
* completed projects (at least 3 projects), similar to this, in which experts involved in the provision of services have participated in the last 3 years;
* valid licenses from SSSCIP for the provision of services in the field of cryptographic (other than electronic digital signature services) and technical information protection according to the list set out in [Appendix 3](#_Appendix_3._The) of this TOR;
* special permit for carrying out activities associated with state secrets. The classification level specified in the special permit must correspond to the classification level for the information to be used during the ARMA ITS inspection;
* confidential records unit within its structure;
* sufficient number of qualified and certified experts to conduct the ARMA ITS examination, which is evidenced by relevant contracts executed with such experts.

The Contractor shall be required to provide information about the experts engaged in the provision of services, namely: a list of documents evidencing their qualifications in the relevant field and the grounds for the provision by them of respective services.

Experts engaged in the conduct of the ARMA ITS examination, during which state secrets are to become known to them, must be provided with duly executed security clearances for access to state secrets. The form of such security clearance must correspond to the classification level of the information that such experts are allowed to access (stipulate their access).

Experts engaged in the conduct of the ARMA ITS examination must hold appropriate educational and qualification degrees, including:

* university degree in the “Information Systems” and/or “Information Technologies” field of knowledge, or a relevant university degree in engineering, or at least three years of proven experience in the field of IT;
* university degree in the “Information Security” field of knowledge, or a relevant university degree in engineering, or at least three years of proven experience in the field of information security.

The Contractor shall be required to sign an agreement on non-disclosure of confidential information that will become known to it during the ARMA ITS examination.

# Appendix 3. The list of licenses from SSSCIP

1. **The license in the field of technical information protection:**

The license for the pursuit of economic activity of provision of services in the field of cryptographic (other than electronic digital signature services) and technical information protection according to the list defined by the Cabinet of Ministers of Ukraine, as regards the assessment of information protection.

1. **The license in the field of cryptographic information protection:**

The license for the pursuit of economic activity of provision of services in the field of cryptographic (other than electronic digital signature services) and technical information protection according to the list defined by the Cabinet of Ministers of Ukraine, as regards the following:

* developing and drawing up a design and other technical documentation, production of cryptosystems and cryptographic information protection facilities (with the right to pursue activities in the field of cryptographic protection of privileged information);
* supply, installation (deployment), configuration, technical maintenance (support), repair and/or disposal of cryptosystems and cryptographic information protection facilities (with the right to pursue activities in the field of cryptographic protection of privileged information);
* topic and expert studies of cryptosystems and cryptographic information protection facilities (with the right to pursue activities in the field of cryptographic protection of privileged information).