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.

2. 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.

3. 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).

3.1. 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.

4. 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.