SCOPE OF WORK FOR INTELLIGENT TRAFFIC MANAGEMENT SYSTEM AT YAHODYN BORDER CROSSING POINT

CONTENTS

OVERVIEW

Introduction

The Intelligent Traffic Management System (ITMS) at the Yahodyn Border Crossing Point (BCP) is intended to automate and streamline vehicle flow, significantly enhancing efficiency and reducing wait times. By integrating advanced traffic monitoring, control technologies, and real-time data analytics, the system optimizes the processing of vehicles, ensuring smoother transitions through the BCP. Key features include automated vehicle identification, dynamic lane assignment, and real-time traffic information dissemination, which collectively improve the overall customer experience for drivers. This system not only expedites the border crossing process but also enhances security and operational effectiveness, contributing to a more efficient and user-friendly BCP.

The scope of the ITMS encompasses the design, development, installation, and handover of an integrated solution to automate vehicle flow. This includes the deployment and approval of technical documentation, development of software and integrating it with existing databases and other relevant Government of Ukraine (GoU) software products, installation of equipment, commissioning of the system, and training for State Customs Service of Ukraine (SCSU) staff on the operation and maintenance of the system. Considering the sensitivity of the information collected and processed ITSM should be designed and developed up to the highest cyber security standards.

System Description

A. The ITMS is being developed considering the perspectives of the Customs and is based on principles that reflect the main requirements for the functioning of the ITMS:

- The operation of the ITMS is carried out on legal grounds and per the legislation of Ukraine.
- A high-tech and efficient ITMS is built on centralized coordination and management of all its components and elements. Such coordination is ensured by the presence of a single management center.
- ITMS information is used both for making operational decisions and for tactical planning based on its analysis.
- The preparedness of the ITMS within the IPCA to reflect and record violations and current processes simultaneously in real-time on the controlled territory.
- The use of intelligent components of the ITMS to ensure the implementation of IPCA functions regarding informing about possible violations.

B. The ITMS is created considering the need to receive, process, and accumulate information from all CI, where customs control and clearance is carried out, and the adjacent territory necessary to ensure proper customs control and CIIP functionality.

C. The ITMS should encompass the areas where customs and border control, clearance of goods, commercial vehicles crossing the customs border of Ukraine, goods and vehicles under customs control, and adjacent territories are located.

D. Upon entry/exit to/from the territory where the ITMS is installed, there must be informational boards with the inscription "VIDEO CONTROL IN PROGRESS.

E. The ITMS should perform the following functions:

- Monitoring the movement of goods and commercial vehicles within controlled territories (Road BCP) in real-time mode. Control should be carried out by recognition of license plate numbers of

vehicles and trailers/semi-trailers upon entry/exit to/from controlled territories and while moving within the controlled territory, as well as through photo and video recording.

- Analysis of workload at the workstations of customs and border officials, as well as controlled sections of the border crossing point (video analytics).
- Traffic management according to established algorithms.
- Outputting the results of ITMS to the Monitoring Center of the Customs.

F. The ITMS must have the following main capabilities and functions:

- Multilevel password protection to control access to video information and Multifactor Authentication.
- Ability to store video information according to specific criteria.
- Capability to work with a multilevel interactive map of the territory (country, region, road BCP).
- Storage of data on recognized license plates, including date and time of recognition, its textual value, and photo of the recognized plate, and vehicle).
- Provision of video footage upon request of the recognized vehicle license plate (frame at the moment of license plate recognition).
- Monitoring of the workload of workstations for personnel of controlling authorities in designated areas of the checkpoint (controlled districts).
- Control of compliance with algorithms.
- Monitoring the status of ITMS components (video cameras, video servers) from remote operator workstations.
- Based on the server platform.

G. The ITMS should have the following analytical capabilities and functions:

- Providing the ability to analyze issues both in real-time mode and by analyzing archived cases.
- Ensuring analysis of the vehicle database.
- Providing the ability to connect third-party vehicle databases.
- Enabling search across connected databases by vehicle number.
- Monitoring the time of vehicles' presence in specified controlled areas at BCPs.
- Software management of controlled territories.
- Visual and auditory notification of ITMS operators about violations of established prohibitions and restrictions in controlled areas.
- Visual and auditory notification of ITMS operators about the presence/absence of queues of vehicles at entrances to controlled areas.
- Preparation of reporting documentation.
- Managing the database of the License Plate Recognition System (LPRS).
- Monitoring vehicle movement in controlled areas (monitoring vehicles' passage through customs formal procedures at BCPs), namely:
  - Entry into the territory.
  - Border control.
  - Weighing.
  - Waiting areas control.
  - Scanning.
  - Customs control and clearance.
  - Inspection of vehicles in enhanced inspection areas.
  - Duration of stay within the territory.
  - Exit from the territory, etc.

H. The Intelligent traffic management system should integrate with the following systems:

- LPRS License Plate Recognition System.
- Access control and Management System.
- VWS Vehicle Weighting System.
- Scanning Systems.
- IPCT.

- The electronic queue for border crossing “E- Queue”.
- Information and telecommunication system of border control “Gart-1”.
- Other systems (if needed).

Definitions and Abbreviations

Intelligent Traffic Management System– the set of technical, software, and mathematical means, including mechanisms of semantic/logical inference, for management procedures and a knowledge base for video monitoring knowledge, which will enable monitoring from the control center of the passage of vehicles through control procedures at the BCPs in real-time mode that are as well components of integration.

An Automated System is a system that consists of personnel and a complex of automation tools to carry out its activities and implements information technology to perform established functions.

The Automated Customs Clearance System “CENTR” is a subsystem that is part of the Unified Automated Information System, enabling the use of electronic documents and copies by the Customs Officers of the State Customs Service for corresponding customs procedures.

Video Analytics is a technology that utilizes computer vision methods for the automated acquisition of various data based on the analysis of a sequence of images captured by video cameras in real-time or from archived recordings.

Arrival Area (Ukraine) – a specially designated area at the BCP for transport interchange, containing a complex of buildings, facilities, and technical means for border, customs, and other types of control and admission of people, vehicles, goods, and other property from the territory of the neighboring state into the territory of Ukraine.

Departure Area (Ukraine) – a specially designated area at the BCP for transport interchange, containing a complex of buildings, facilities, and technical means for border, customs, and other types of control and admission of people, vehicles, goods, and other property from the territory of the neighboring state into the territory of Ukraine.

Single Automated Information System – a multifunctional integrated automated system that provides informational support and maintenance of State Customs Affairs in Ukraine, consisting of several interconnected information systems, including the automated information system “Center”, the telecommunications system “E-mail”, and other software-information complexes.

User Identifier is a certain device or attribute by which the user is determined. Identifiers can be contactless proximity cards, magnetic cards, Touch Memory key fobs, various radio key fobs, iris images, fingerprints, palm prints, and many other biometric features. A specific unique binary code characterizes each identifier. In an access control system, information about the rights and privileges of the identifier owner is assigned to each code.

Integration Components – individual objects of customs infrastructure, their geographical or functional combination, technical means of customs control, information resources, intelligent traffic management systems, vehicle traffic management tools, etc., which are installed on controlled territory or used during customs formalities, interacting with each other through an integration platform of controlled territory and a centralized integration platform for automating customs procedures.

Integration Platform of Controlled Territory (IPCT) - Structural component of integration of Intelligent Platform Management Interface (IPMI), which ensures:

- Interaction of Customs infrastructure objects, information resources, technical means of Customs Control, intelligent traffic management system, traffic management tools, etc., (Integration components) for automation of customs procedures.
- Acceleration of customs clearance and customs control procedures without compromising their effectiveness and efficiency by excluding or reducing the manual data.
- Traffic management system within the controlled territories.

Intelligent Platform Management Interface (IPMI) for Customs Infrastructure – dual information and telecommunication system (hereinafter – the System) which:

- It represents a set of proprietary technical, software, and logical-mathematical tools that are managed and stored in the memory of such a system.
- Ensures interaction of information resources, technical means of customs control, intelligent traffic management systems, traffic management tools, etc., (Integration components) installed at the controlled territory.
- Designated to support the activities of Customs Officials, in certain situations both in advisory and in automatic modes according to a predefined scenario.

IPMI dual structure consists of:

- A centralized integration platform.
- Integration Platform of Controlled Territory (IPCT).

The Head of the Customs Clearance Department or acting – is an official of the customs office who, per the established procedure, is appointed as the head of the Customs Clearance Department, or to whom, according to the job description, the duties of the Head of the Customs Clearance Department are entrusted within the corresponding period.

Monitoring Center – a structural subdivision of the Customs authority and/or personnel as per the established procedures authorized to implement specific (special) functions, as well as Customs Officials who carry out the following:

- Monitoring implementation of customs procedures.
- Implementation of measures in the field of combating smuggling and violations of customs regulations; prevention and counteraction to manifestations of corruption, bribery, and other abuse of power within the Customs Service.
- Monitoring the operability of integration components (breakdown, malfunction, unjustified exclusion, etc.).
- Response to incidents in the field of Customs Affairs.

Customs Infrastructure (CI) - the territory (location), administrative and technological buildings and facilities, equipment, stationary, technical, and special means of Customs Control, information systems and resources, information and telecommunication networks, data processing centers, etc., used for customs and clearance, as well as other functions carried out by Customs Authorities, and for which regulatory or administrative acts in customs matters establish requirements for their establishment (arrangement) and functioning.

Customs infrastructure includes:

- Border Crossing Points (hereinafter – BCPs).

- Control Points (hereinafter – CP).
- Scanning systems.
- Weighing complexes, etc.

Road Border Crossing Points (controlled territory) – specially designated areas on roadways with a complex of buildings, structures, and technical facilities, where border, customs, and other types of control and passage through the state border of individuals, vehicles, goods, and other property are carried out, and which is equipped per the requirements approved by the Resolution of the Cabinet of Ministers of Ukraine dated August 17, 2002, No. 1142.

A neighboring state is a country that shares a part of its border with Ukraine.

Vehicle Weighting System comprises technical and software tools that provide processing of information related to vehicle weighing, enabling effective weight control of vehicles within the premises.

License Plate Recognition System comprises technical and software tools that provide reading and recognition of vehicle license plates, as well as storage of information regarding video monitoring for the purpose of operational monitoring of vehicles moving through control areas within the territory of the facility.

Access Control and Management System comprises technical and software tools used to address the tasks of controlling and managing access to specific premises and territories, as well as to provide real-time monitoring of personnel movement and their time spent in the premises of the facility.

The scanning system comprises technical and software tools that provide scanning of vehicles, transmission, and storage of the results, through which control of the content of vehicles is carried out by applying non-intrusive methods.

Tampering (anti-sabotage) – is an alarm system for the continuous monitoring of the equipment's operability to detect technical malfunctions, as well as unauthorized interference in the video monitoring system (such as lens contamination, image darkening or overexposure, camera rotation or disconnection, etc.).

A Vehicle is a road means of transportation designated primarily for use on public roads of all categories and constructed according to the State Standard of Ukraine 2984-95).

Air Raid Alert – is an informational message generated, according to specified visual and/or auditory parameters. These alerts can be communicated through various means, including sirens, loudspeakers, radio broadcasts, television, and digital notifications etc.

Functional Module "Customs Control Area Dispatcher" is a component of the automated customs clearance system "CENTR" used for registering and accounting for goods and vehicles moving through the customs border of Ukraine at the checkpoint using "red corridor" lanes, obtaining real-time information on their location and time spent in the customs control zone, generating registers of vehicles under customs control during shift handovers between customs clearance units.

The queue of vehicles is a group of vehicles that are located before the entrance to the Road BCP and waiting to enter its territory.

Centralized Integration Platform (CIP) a structural component of CIIP integration, which provides:

- Implementation of the function of the Monitoring Center of the State Customs Service of Ukraine.
- Centralized coordination and management of all connected integration platforms of controlled territories.

Critical equipment - the list of equipment that is determined by vendor as critical and without which the functioning of the ITMS is impossible. This list must be approved by USAID ERA and SCSU in the stage “System Design”.

Common abbreviations:

Customs – State Customs Service of Ukraine.

Customs MC – Monitoring Center of State Customs Service of Ukraine.

CIIP – Customs infrastructure integration platform.

IPCT – Integration Platforms of Controlled Territories.

CIP – Centralized Integration Platform.

CI – Customs Infrastructure.

SW – Software.

Road BCP – Road Border Crossing Point for Vehicles.

V – Vehicle.

ITMS – Intelligent traffic management system.

LPRS – License Plate Recognition System.

ACMS – Access Control and Management System.

VWS – Vehicle Weighting System.

SS – Scanning System.

ACCS "CENTR" – Automated Customs Clearance System "CENTR".

FM CCAD – Function Module "Customs Control Area Dispatcher".

SCOPE OF WORK: SERVICES

Design Development

The vendor is required to develop and get approval from the State Customs Service of Ukraine (SCSU) for the design of the Intelligent Traffic Management System (ITMS) at the Yahodyn BCP, ensuring alignment with the technological requirements and equipment specifications outlined in this Statement of Work (SoW). The vendor's deliverables include:

1. **Predesign Information Collection:** Gather all necessary predesign information to inform the system design.

2. **Technical Documentation:** Create comprehensive technical documentation for the ITMS, including detailed specifications and installation guidelines.

3. **Approval Securing:** Obtain required approvals from the SCSU and other relevant authorities for system integration.

4. **Design Solution:** Provide a comprehensive design solution that complies with all applicable regulations and standards, ensuring high quality and precision through rigorous quality control measures.

5. **Design Revisions:** Be prepared to revise the design based on feedback from the project team and Customs officials, thoroughly addressing all concerns and requirements.

These deliverables are critical to ensuring the successful implementation and integration of the ITMS

The vendor shall collaborate closely with the project team and the State Customs Service of Ukraine officials to ensure the design meets operational and regulatory requirements. The vendor should also consult other authorities where data integration is required for other government systems and maintenance of the equipment.

Scope of the Design Task

The selected vendor will be responsible for delivering the following design services:

i. Site Assessment and Pre-Design Tasks

Conduct a thorough site assessment of the Yahodyn BCP to gather all necessary data regarding current traffic flow, infrastructure, and potential locations for ITMS components. Including an assessment of system integration and data-sharing needs with other software products currently used at the BCP, ensuring seamless interoperability.

After the assessment and before completing the detailed design, the vendor shall organize and deliver a presentation of the site assessment findings and the proposed solution / high-level design to the GoU stakeholders from SCSU, SARDI, MOR, and SBGSU.

ii. System Design

Develop a detailed design of the ITMS, addressing the following elements:

- Monitoring Cameras: Positioning for optimal coverage of all traffic lanes and critical areas.
- Automated Barriers: Locations and types suitable for controlling vehicle access.
- Traffic Lights: Placement and integration with control systems to manage vehicle flow.
- Operators working stations and Server: Location and connection to the system.
- Communication and Data Transmission Systems: Ensuring reliable connectivity between all system components.
- Power Supply Systems: Design of primary and backup power solutions to ensure uninterrupted operation.

Ensure the design adheres to all relevant Ukrainian regulations and international best practices for traffic management and security systems. In particular, the vendor should comply with following standards:

- DBN A.2.2.3 2014 - Composition, procedure for development, coordination, and approval of project documentation for construction;
- DSTU B A.2.4-4:2009 - Basic requirements for project and working documentation;
- ISO/IEC 11801:Ed 2.2:2011-06 - Information technology – Generic cabling for customer premises – Edition 2.2 (June, 2011);
- ISO/IEC 14763-2 Edition 1.0: 2012 - Information technology. Implementation and Operation of Customer Premises Cabling. Part 2: Planning and Installation (February, 2012);
- EN 50174-2 (2009) - Information Technology - Cabling installation - Part 2. Installation planning and practices inside buildings;
- ANSI/TIA-568-C.0:2009 - Generic Telecommunications Cabling for Customer Premises (February, 2009).

Detailed Design Deliverables:

The vendor must include the following as part of its design work.

Prepare and submit detailed design documentation, including:

- Site assessment report with high level design summary (see task desicription above).
- Design drawings, schematics, diagrams, and documentation.
- Technical specifications for all equipment
- Installation guidelines and requirements
- Bill of Quantities (BoQ)

For the Schematic Diagram, the vendor should:

- Provide a comprehensive schematic diagram illustrating the integration and layout of all ITMS components.
- Ensure the design diagram includes clear labeling and descriptions of each element.
- Present the design to State Customs and other stakeholders/users.

For the Bill of Quantities the vendor must include:

- Equipment and Materials; the BoQ should detail all equipment and materials necessary for the ITMS.
- Installation Works; the BoQ should also include a detailed breakdown of all labor associated with the installation of the ITMS components.

The vendor should follow the following design approval process:

- The vendor shall collaborate with the project team and the SCSU officials to review and refine the design as needed.
- Obtain formal approval from the USAID ERA project team and Customs before submitting the final design for building inspection approval.
- Submit final design for billing and payment to USAID ERA (note all payments will be made by DAI upon approval by both the project team and the State Customs).

Detailed Requirements: System Installation and Commissioning (Yahodyn)

General Requirements

It is necessary to install the equipment, namely:

- delivery of equipment at the address: Volyn region, Kovelsky district, village Starovoytove, str. Prykordonnikiv, 2.
- installation and connection of the power supply system in the server room and monitoring center.
- assembly of server telecommunication cabinets.
- installation of servers in telecommunication cabinets.
- connection of communication channels 2 x 10 Gbit/sec.
- lay of a structured cable network and inclusion of equipment in it.
- installation, connection, and adjustment of ACS equipment.
- installation, connection, and adjustment of equipment in operators' workplaces.
- installation, connection, and configuration of video cameras.
- configuration of the servers of the international checkpoint video control system for road traffic.
- conducting tests.

Requirements of ITMS installation at a road BCP

Entry into Ukraine

Entry into the BCP from the territory of a bordering state:

- monitoring video cameras to control the queue at the entrance to the BCP, video cameras for recognition of front and rear license plates of vehicles (the number depends on the number of traffic lanes for entering the BCP at the rate of two video cameras for each traffic lane) and a barrier (the number depends on the number of traffic lanes for entering the BCP, based on the calculation of one barrier in each traffic lane);
- video cameras that cover the waiting areas, an electronic board with traffic lanes (cargo, passenger, green, red).
- Large easily readable sign should be installed at the entrance informing drivers and passengers about video monitoring and recording at the BCP territory.
- There must be a possibility of installing portable equipment at the BCP (automated workplace or Terminal with software and equipment for wireless data transmission over secure VPN communication channels to ensure at the entrance to the checkpoint control from portable equipment barriers (opening/closing) with IP controllers installed on them.

i. “Green” corridor (passenger direction)

- the area of waiting for control procedures: monitoring and robotic video camera to control the situation.
- the area of control procedures: monitoring video cameras, video cameras for recognition of front and rear license plates of vehicles (the number depends on the number of traffic lanes, and a traffic arm (the number depends on the number of traffic lanes for entering the traffic control system, one traffic arm per lane)

ii. “Red” corridor (cargo and passenger directions)

- weighing complex: a video camera for recognition of the front number plates of the vehicle before entering the weighing platform (the number depends on the number of installed weighing complexes in the territory of the entry to Ukraine, based on the calculation - one video camera for each weighing complex) and traffic lights at the entrance to the weighing platform and exiting the weighing platform (the number depends on the number of installed weighing complexes in the territory of entry into Ukraine, based on the calculation of two traffic lights at each weighing complex, a monitoring video camera to ensure video control of the weighing process;
- Border control area: monitoring video camera for supervision of border control actions.
- Area of waiting for customs clearance, cargo/passenger directions: monitoring and robotic video camera to control the situation.
- the area of customs control of passenger/cargo directions: monitoring video cameras, video cameras for recognition of the front and rear license plates of vehicles (the number depends on the number of traffic lanes, and the traffic arm (the number depends on the number of traffic lanes for entering the BCP, based on the one traffic arm on each traffic lane);
- stationary (mobile) SS: video camera for recognition of the front number plates of vehicles at the exit from the SS (the number depends on the number of installed scanning systems in the territory of entry into Ukraine, based on the calculation of one video camera for each scanning system), monitoring video camera to ensure video control of scanning process.
- customs control zone: monitoring video camera to ensure video control of the process of passing customs control by persons and vehicles moving across the state border (the number depends on the number of traffic lanes for vehicles in the customs control zone on the territory of entry into Ukraine, at the rate of one a video camera on each traffic lane) and a traffic light at the entrance to the customs control zone (the number depends on the number of lanes for the movement of vehicles in the customs control zone on the territory of the entrance to Ukraine, one in each traffic lane);
- premises in which customs officials of the State Customs Service and the State Border Service carry out control procedures: monitoring video cameras to ensure video control of the process of control procedures carried out by officials of the State Customs Service and the State Border Service (the number depends on the area of the premises and the number of workplaces for officials persons);
- leaving the customs control zone: a video camera for recognition of the front number plates of vehicles (the number depends on the number of traffic lanes for vehicles in the customs control zone on the territory of entry into Ukraine, based on one video camera for each traffic lane, traffic arm (the number depends on the number of traffic lanes for motor vehicles in the customs control zone on the territory of entry into Ukraine, one in each traffic lane)

a. Area for waiting for exit from BCP in cargo and passenger directions:

- monitoring video camera.

iii. Exit from the BCP to the territory of Ukraine:

- video cameras for recognition of front and rear license plates of vehicles (the number depends on the number of traffic lanes for exiting the APA, based on two video cameras for each traffic lane); and
- a traffic arm (the number depends on the number of lanes for the exit of the vehicle) from the territory of the APP, at the rate of one in each traffic lane.

Exit from Ukraine

i. Entry into the BCP from the territory of Ukraine:

- monitoring video cameras to control the queue at the entrance to the APA, video cameras for recognition of front and rear license plates of vehicles (the number depends on the number of

traffic lanes for entering the APA, based on the calculation of two video cameras for each traffic lane); and

- a traffic arm (the number depends on the number of traffic lanes for entering the APP, based on the calculation of one traffic arm in each traffic lane);
- video cameras covering the waiting areas, an electronic scoreboard with traffic lanes (freight, passenger, green, red).
- Large easily readable sign should be installed at the entrance informing drivers and passengers about video monitoring and recording at the BCP territory.
- At the checkpoint, provide for the possibility of installing portable equipment (automated workplace or Terminal with software and equipment for wireless data transmission over secure VPN communication channels to ensure control of barriers from portable equipment at the entrance to the checkpoint (opening/closing) with IP controllers installed on them.

ii. Cargo terminal and lanes

- Weighing complex cargo directions: a video camera for recognition of the front license plates of the vehicle before entering the weighing platform (the number depends on the number of installed weighing complexes in the territory of departure from Ukraine, based on the calculation of one video camera for each weighing complex),
- traffic lights at the entrance to the weighing platform and exit from the weighing platform (the number depends on the number of installed weighing complexes in the territory of departure from Ukraine, based on the calculation of two traffic lights at each weighing complex); and
- a monitoring video camera to ensure video control of the weighing process;

a. the area where border control is carried out:

- monitoring video camera for video recording of control actions.
- waiting area for customs clearance: monitoring and robotic video camera to control the existing situation.

b. the area where customs control is carried out:

- video camera of the "Fish eye" type, monitoring video camera to ensure video control of the process of passing customs control by persons and vehicles moving across the state border (the number depends on the number of traffic lanes for vehicles in the customs control zone on the territory of entering Ukraine, at the rate of one video camera in each traffic lane); and
- a traffic light at the entrance to the customs control zone (the number depends on the number of lanes for vehicle traffic in the customs control zone at the entrance to Ukraine, at the rate of one on each traffic lane);

c. premises in which officials of the Customs Service of the State Customs Service and the State Border Service carry out control procedures:

- monitoring video cameras to ensure video control of the process of implementation of control procedures by officials of the Customs Service of the State Customs Service and the State Border Service (the number depends on the area of the premises and the number of workplaces placed in it for employees);

d. leaving the customs control zone:

- a video camera for recognition of the front number plates of vehicles (the number depends on the number of traffic lanes for vehicles in the customs control zone on the territory of entry into Ukraine, based on one video camera for each traffic lane); and
- traffic arm (the number depends on the number of traffic lanes for motor vehicles in the customs control zone on the territory of entry into Ukraine, one in each traffic lane).

iii. **Passenger direction**

a. waiting area for control procedures:

- monitoring and robotic video camera to control the situation.

b. the area where control procedures are carried out (border and customs control):

- "Fish eye" video camera, monitoring video camera to ensure video control of the process of passing customs control by persons and vehicles moving across the state border (the number depends on the number of traffic lanes for vehicles in the area of control procedures on the territory of departure from Ukraine, based on the calculation of one video camera in each traffic lane); and
- traffic lights at the exit to the customs control zone (the number depends on the number of lanes for the movement of vehicles in the customs control zone on the territory of departure from Ukraine, based on - one on each traffic lane).

c. premises in which customs officials of the State Customs Service and the State Border Service carry out control procedures:

- monitoring video cameras to ensure video control of the process of control procedures carried out by officials of the State Customs Service and the State Border Service (the number depends on the area of the premises and the number of workplaces placed in it for officials).

d. a departure from the customs control zone (for passengers):

- video camera for recognition of the front license plates of vehicles (the number depends on the number of traffic lanes for vehicles in the customs control zone on the territory of exit from Ukraine, based on the calculation - one video camera for each traffic lane),
- barrier (the number depends on the number traffic lanes for motor vehicles in the customs control zone on the territory of entry into Ukraine, at the rate of one per traffic lane); and
- a reader of service cards of officials of the State Customs Service installed on the traffic arm (the number depends on the number of installed traffic arms, at the rate of one at each traffic arm), which should provide control of the opening of the traffic arms installed at the exit from the customs control zone in "manual mode".
-

e. area of BCP for waiting for departure from the cargo and passenger directions:

- monitoring video camera.

f. exit from the BCP to the territory of a neighboring state:

- video cameras for recognition of front and rear license plates of vehicles (the number depends on the number of traffic lanes for exiting the APA, based on two video cameras for each traffic lane); and
- a barrier (the number depends on the number of traffic lanes for the exit TZ from the territory of the APP, based on the calculation - one in each traffic lane.

iv. Territory of road BCP –

- video cameras for recognition of license plates of vehicles, robotic video cameras to ensure the possibility of detailed video control in the BCP (the number depends on the area of the BCP, but not less than two),
- monitoring video cameras (the number depends on the control zones in the BCP) and readers (service cards of officials of the State Customs Service and the State Border Service)
- Control systems and access control (the number depends on the number of places with controlled access), including:
- in-depth inspection box: monitoring video cameras and ACMS readers (two or more video cameras in each box to provide a detailed 360-degree view of the box room and two readers for each gate).

a. parking lot of detained vehicles:

- monitoring video camera (the number depends on the area of the parking lot).

b. server room:

- monitoring video camera and 2 ACMS readers for entry and exit (the number depends on the number of server rooms).

c. gate in the fence delimiting the entry and exit zones in the BCP for turning around the vehicle in the event of its return to the territory from which it arrived:

- monitoring video camera and 2 ACMS readers for each gate.

d. gates in the fence delimiting the entry and exit zones in the APP:

- ECU readers, etc.

An example of the procedure for exiting Ukraine through passenger and cargo lanes is given in Annex 2.

Requirements for installation of server and telecommunications equipment

Server and telecommunication equipment must be installed in a separate room of the service and production building of the BCP. The equipment must be placed in a separate, specially equipped server room (hereinafter referred to as the server room), consisting of areas for placement of:

- server and telecommunication equipment.
- devices of the power supply system.
- equipment of microclimate support systems, technical electrical safety, technical information protection, and other equipment.

These premises must be equipped with the following systems:

- access control system.
- video monitoring system.
- autonomous power supply system.
- fire alarm system.
- climate control system (ventilation, temperature, humidity).
- structured cable system.

Passages in front and behind the equipment must provide free access and be at least 80 centimeters.

The presence of people in the server room permanently (use of the room as an office) is not allowed. Also, the use of server premises as warehouses for storing documents, tools, materials, telecommunications, and informatization facilities, etc. is not envisaged.

It is not recommended to locate sources of electromagnetic radiation (devices for accessing telecommunication networks based on Wi-Fi, GSM, CDMA technologies, etc.) in the server room, which can negatively affect the operation of the server and telecommunication equipment.

The installation of the walls (partitions) and doors of the server room must be airtight. The walls, ceiling, and floor should be flat, without protrusions and overflows, and have a coating that makes it difficult for dust to separate, settle, and accumulate on the surface. Materials should not release and accumulate dust and should not accumulate electrostatic charge.

- Building materials used for installation should be selected with properties to minimize mold growth and rodent damage.
- Surfaces should be light to improve the overall lighting of the room.

The materials used in the improvement of the premises must comply with sanitary standards and fire safety rules:

- by flammability groups.
- by the spread of fire.
- by smoke-forming ability.
- toxicity of combustion products and flammability per the fire resistance category.

Ceilings must be waterproofed to exclude the possibility of water leaking into the server room.

It is not recommended to use a suspended (false) ceiling in the server room.

The server room must be equipped with an antistatic linoleum floor.

The microclimate system consists of subsystems of ventilation (if necessary) and air conditioning.

The structured cable system consists of:

- subsystems of cable communications organization.
- sub-systems for placement of assembly cabinets.

The fire protection system consists of a fire alarm system.

- According to DBN B.2.5-56, the server room must be equipped with a fire alarm system, the type of system equipment used, and the location of sensors are determined at the stages of operational design per the requirements of DBN B.2.5-56, DSTU EN 54-14, DSTU EN 54-13.
- The server room is not subject to equipment according to DBN B.2.5-56 with automatic gas fire extinguishing systems, it must be equipped with primary fire extinguishing means (mobile or portable gas fire extinguishers).

Climatic conditions in server rooms are characterized by the following indicators: air temperature and relative air humidity. In the server room, it is necessary to control the temperature and humidity so that they are constantly within the recommended operating ranges according to DSN 3.3.6.042-99 and ANSI/TIA-942-A:

- air temperature: from 20ºC to 25ºC.
- relative air humidity: from 40 % to 60 %.

The air conditioning system must ensure uninterrupted operation in the event of a loss of the primary power supply of the server room or at the time of input switching or start-up of a backup gasoline or diesel power plant.

Local network switches of individual nodes that connect to network equipment in the server room should be placed in specialized server cabinets with locks.

Subscriber access telecommunications equipment is installed in telecommunication cabinets with locks, which are placed on the floors of buildings in corridors or separate rooms and are powered by a backup (guaranteed) power supply system.

Server rooms are classified as regular rooms. The list of persons who have access to these premises should be determined by internal orders. The time and purpose of visits of all persons who enter the premises must be registered in the logbook.

Detailed Requirements: Equipment Installation and Commissioning (Kyiv)

Assembly of the equipment:

- transportation of equipment to the address:11G Dehtiarivska Str., Kyiv.
- installation and connection of the power supply system in the server room and monitoring center.
- assembly of server telecommunication cabinets.
- installation of servers in telecommunication cabinets; - connection of communication channels 2 x 10 Gbit/sec.
- installation of a structured cable network for connection of equipment.
- assembly, connection, and adjustment of equipment ACS.
- -assembly, connection, and adjustment of equipped workplaces for operators.
- installation, connection, and adjustment of video cameras.
- adjustment of ITMS servers at the international road BCP;
- testing
- provision of test logs and reports.

Detailed Requirements: Training and Handover

Training Program Requirements

The vendor shall develop and implement a comprehensive training program for Customs officials to ensure they can effectively operate and perform basic maintenance on the ITMS components, including cameras, networks, and software. During the design phase, the vendor must first assess the current capabilities of the Customs staff who will be involved, identifying specific knowledge gaps. Based on this assessment, the vendor will design a tailored training program that addresses these gaps and meets the needs of the staff. The Customs staff and technicians should be involved from the start during the design phase, and their assessment should be done early in the process to allow time for adequate planning for the availability of resources, qualifications, and time commitments from the staff.

The training should be conducted before system commissioning and should prioritize an on-the-job training approach to provide practical, hands-on experience. The training program must also include a comprehensive module on cybersecurity, covering secure system access and data transfer protocols. The training should also include troubleshooting, support, and maintenance protocols and documentation. Upon completion of the training, each participant should receive a certificate detailing the topics covered and the number of training hours completed.

Starting with the design phase, the vendor should employ a change management methodology to evaluate the impacts of the Customs business processes and impacts on people. The training, transition into operation, and organizational change management should be part of the overall plan to ensure a successful transition into operation and transition of ownership to the beneficiary.

System Handover Requirements

The vendor shall ensure a smooth and comprehensive handover of the Intelligent Traffic Management System (ITMS) to the State Customs Service of Ukraine upon project completion. This process will include a detailed handover plan that covers the transfer of all system documentation, user manuals, technical specifications, and maintenance guidelines. There will be quantity acceptance for items, devices, and software delivered, and after implementation, there should be quality acceptance of the

working system. The quality acceptance could be delayed by one month to ensure that both the systems are performing as intended and people are able to manage and operate the system.

The vendor must conduct a final system walkthrough with designated Customs officials, demonstrating the operational capabilities and maintenance procedures of all ITMS components. Additionally, the vendor shall provide a full inventory of all installed equipment, ensuring that everything is correctly labeled and documented. Any outstanding issues or defects must be resolved before the handover is finalized. A formal handover report, signed by both the vendor, USAID ERA, and the State Customs Service of Ukraine, will confirm the successful transfer of the system. The vendor shall also offer post-handover support for a specified period to address any initial operational issues or questions.

Deployment and System Warranty Period

The vendor is required to provide a Deployment and System Warranty period of six months following the initial deployment of the ITMS. During this period, the vendor shall offer comprehensive support and maintenance services to ensure the system operates smoothly and meets all specified requirements. The following obligations are included within this warranty period:

- Adjustments and Fine-Tuning: The vendor shall make any necessary adjustments to optimize the system's performance and ensure it aligns with the operational needs of the State Customs Service of Ukraine (SCSU).
- Configuration Changes: Any additional configuration changes required to enhance system functionality or to adapt to evolving operational requirements shall be implemented by the vendor at no additional cost.
- Error Corrections: The vendor must promptly address and correct any software bugs, hardware malfunctions, or system errors that are identified during the warranty period.
- Technical Support: The vendor shall provide ongoing technical support, including troubleshooting assistance and guidance on system usage, to ensure continuous and efficient operation of the ITMS.
- Documentation Updates: Any necessary updates to the system documentation resulting from adjustments or corrections made during the warranty period must be provided to SCSU.

This six-month Deployment and System Warranty period ensures that the ITMS is fully functional and optimized for the specific needs of the Yahodyn BCP, providing SCSU with confidence in the system's reliability and performance.

Transfer of Software Rights

The vendor is required to transfer all rights to the developed ITMS software to the State Customs Service of Ukraine (SCSU) upon project completion. This includes providing SCSU with full ownership of the software, including source code, documentation, and any associated intellectual property. The transfer must ensure that SCSU holds perpetual rights to use, modify, and distribute the software without any restrictions or additional licensing fees. The vendor must also supply comprehensive technical documentation and training to enable SCSU to maintain and update the software independently. This transfer of rights will be formalized through a legally binding agreement, ensuring that all proprietary and usage rights are clearly and unambiguously conveyed to SCSU.

Detailed Requirements: Maintenance and Warranty

The vendor shall sign a contract for the maintenance of hardware components for three years and five years of software maintenance and support. During this period, the vendor will be responsible for ensuring the optimal performance, reliability, and longevity of the Intelligent Traffic Management System (ITMS) at the Yahodyn Border Crossing Point (BCP). The points below outline the specific requirements and obligations that the vendor must fulfill under this maintenance contract.

The maintenance contract is designed to ensure the long-term reliability and efficiency of the ITMS, providing the State Customs Service of Ukraine with the assurance that the system will be supported and maintained to the highest standards throughout the contract period.

1. Maintenance and Inspections

Scheduled Maintenance: The vendor shall provide regular maintenance services, including preventive and predictive maintenance, at intervals agreed upon in the contract. Typically, maintenance should be conducted every six months.

Inspections: Conduct comprehensive inspections of all ITMS components, including cameras, barriers, traffic lights, sensors, communication systems, and power supplies. Inspections should occur at least once a year.

2. Warranty Repairs and Replacements

Warranty Services: The vendor shall provide a three-year warranty for all ITMS equipment, covering manufacturing defects and premature wear and tear. This warranty does not cover misuse or physical damage. The vendor is obligated to provide prompt replacement of faulty components under warranty. The vendor should provide an SLA for defective equipment replacement and an SLA for support. For critical equipment, an on-site 4-hour turnaround time for equipment or component replacements and configuration is required

Component Replacements: Supply and install replacement parts and components as needed, ensuring that all replacements are of equivalent or higher quality than the original parts.

3. System's Support

The vendor should provide information on guaranteed up-time, support response SLAs, and resolution SLAs. If the vendor is not able to honor the SLAs, there should be a deduction in maintenance costs.

The vendor should also provide a support system for logging tickets and a call center or dedicated phone line for priority 1 incidents or major incidents with a 30-minute response time.

4. Software Updates and Upgrades

Regular Updates: Ensure that all system software is kept up to date with the latest patches and updates to maintain security and functionality.

Upgrades: Propose and implement system upgrades as technology advances, ensuring the ITMS remains state-of-the-art.

5. Training and Knowledge Transfer

Ongoing Training: Provide once-a-year refresher training sessions for Customs officials to keep their skills up to date with any system changes or upgrades.

Documentation Updates: Supply updated user manuals and technical documentation whenever significant changes or upgrades are made to the system.

DETAILED SPECIFICATIONS: SYSTEM COMPONENTS' REQUIREMENTS (SOFTWARE & HARDWARE)

General Requirements

ITMS must comply with the following requirements:

I. Number of video channels: not less than 250.
II. Ability to further increase the number of input channels by adding standard video servers, management servers, and switches, and constructing a centralized ITMS in the data processing center capable of scaling up to 100,000 video cameras.
III. Video data retention period: no less than 90 days (in continuous recording mode from all cameras at a resolution of 1920x1080, 25 frames per second), retention period for license plate recognition data – 1095 days.
IV. Support for simultaneous connection of no fewer than 100 operators or analysts, regardless of the number of input channels.
V. Ability to administer the entire system from a single management window.
VI. Provision for building a Wi-Fi network within the territory of the international BCP.
VII. Centralized updating of embedded software versions on video servers operating within the ITMS of the international road BCP.
VIII. The server equipment of the ITMS must be placed in the existing server room, equipped with a fire alarm, security systems, air conditioning, and fire extinguishing systems.
IX. The specification outlined in this SOW provides a minimum acceptable level of performance, Vendors could suggest specific models with parameters not less than stipulated below.
X. Vendors are responsible for developing designs based on the ITMS requirements and providing a final list of equipment required.

Proposals for specific camera installation locations must be coordinated with the Customer after surveying potential installation sites throughout the checkpoint area during the design phase, according to the requirements specified.

Detailed Specifications: Software Requirements

The ITMS software must be designed to integrate seamlessly with the existing systems and databases of the State Customs Service of Ukraine (SCSU). The following outlines the specific requirements for the software:

Integration Capabilities

- **Existing SCSU Systems:** The software must be compatible with and able to integrate seamlessly with the current SCSU systems and databases, ensuring smooth data flow and operational coherence.
- **E-cherha System:** Integration with the E-cherha (E-queue) system, managed by the Ministry of Communities, Territorial Development, and Infrastructure, is required. This integration should

facilitate efficient queue management and enhance coordination at the Border Crossing Point (BCP).

- **SBGSU Guard 1 System:** The software must also integrate with the SBGSU Guard 1 system to ensure comprehensive security management and operational efficiency.

Hardware Compatibility

- **ITMS Hardware:** The software must be fully compatible with all ITMS hardware components, including cameras, sensors, barriers, traffic lights, and communication devices. This ensures optimal performance and reliability of the overall system.

Scalability and Flexibility

- **Scalability:** The software should be designed with scalability in mind, allowing for easy expansion and deployment at additional Border Crossing Points (BCPs) as required.
- **Flexibility:** The system must be flexible to adapt to future technological advancements and changing operational needs.

Cybersecurity and Data Protection

- **Cybersecurity:** Strong emphasis must be placed on cybersecurity measures to protect against threats and unauthorized access. This includes:
  - Data encryption
  - User authentication and access controls
  - Regular security updates and patches
- **PII Safety:** The software must ensure the safety and confidentiality of Personally Identifiable Information (PII), adhering to all relevant data protection regulations and standards.

Network segmentation

Cameras, Access Control, and other networked IOT/ICS devices must be segregated on a physically or logically segregated network from other IT systems. These IOT/ICS devices should not have any direct connection to or from the public internet and should only be accessible from internal networks. These IOT/ICS devices should not have any direct connection to the server or other internal networks except where necessary. All administration interfaces must be accessible only from internal network locations and must be blocked from public access.

Device Passwords

All devices including, network equipment (switches, routers, firewalls), servers, workstations, IOT/ICS, and other devices must have strong unique passwords that are stored in a secure method. No devices should be left with their default password.

Security Testing

All hardware and software must undergo security testing which may include penetration testing, dynamic application security testing (DAST), static application security testing (SAST), or other applicable testing methods. A security report should be provided that highlights all findings and includes raw output from the security tests. Any finding with a rating of high or critical must be resolved before handover.

Software Libraries, Modules, and Frameworks

Any libraries, modules, frameworks, or other components used in custom software development must be up-to-date and actively supported at the time of delivery.

Compliance and Hosting

- **SCSU Policies and Protocols:** The software must comply with all SCSU policies, protocols, and regulatory requirements, ensuring legal and operational alignment.
- **Server Location:** The primary server for the software must be located in Kyiv, providing a centralized and secure hosting environment.
- **Backup and Disaster Recovery Options:** Robust backup solutions must be implemented to ensure data integrity and availability in case of system failures or other emergencies.

Licensing

- **Perpetual License:** The software license should be perpetual, offering long-term use without the need for ongoing renewal fees. This ensures cost-effectiveness and continuous operational capability.

Software Delivery and Acceptance Process

The process of software delivery and acceptance for the ITMS should be organized in a structured and iterative manner to ensure thorough evaluation and continuous improvement. The vendor shall employ an iterative delivery approach, beginning with the development and demonstration of a Minimum Viable Product (MVP). This initial MVP should encompass core functionalities and provide a tangible representation of the software's capabilities.

Upon completion of the MVP, a demonstration should be conducted for the project team and the State Customs Service of Ukraine (SCSU) to gather initial feedback. Subsequent iterations should incorporate this feedback and expand the software's functionality incrementally, with regular review and approval checkpoints. Each iteration should be thoroughly tested, and a formal acceptance test should be conducted at the end of each phase. This iterative approach ensures that the software meets all functional, operational, and security requirements, and allows for early identification and resolution of potential issues.

Final acceptance of the software will be granted once all iterations have been completed, all requirements have been met, and the system has been fully tested and validated by both the project team and SCSU officials.

ITMS software must provide:

- Control of the movement of vehicles within controlled territories (BCPs with ITMS in real-time mode). Control should be carried out by reading and recognizing the license plates of vehicles and trailers/semi-trailers upon entry/exit to/from the controlled territory and during the movement of vehicles through the controlled territory, as well as by photo and video recording of vehicles.
- Transmission of video monitoring results to the monitoring center of the Customs.
- Operation with a multi-level interactive map of the controlled territory (no less than three levels - country, region, controlled area).
- Monitoring the status of components of the ITMS (cameras, video servers, weighing complexes, scanning systems, operators, etc.) from remote operator workstations.
- Based on the server platform.
- Ability to simultaneously display images from multiple cameras, as well as a full-screen display of video information from each camera.

- Ability to assign a textual label to each camera, the label should include the camera number and name, current time, and date.
- Ability to export video information to external storage devices.
- Ability to individually adjust image parameters, compressed image quality, and recording speed for each camera.
- Ability to configure recording modes: motion detection, external air raid alert signal, continuous recording, scheduled recording, and cyclic recording.
- Ability to set the storage time for recordings on the server independently for each camera.
- Ability to analyze issues in real-time mode and by analyzing archived occasions.
- Providing analysis of the vehicle database.
- Monitoring the time spent by a vehicle in controlled areas.
- Visual and auditory notification of the ITMS operator about violations of established prohibitions and restrictions in controlled areas.
- Visual and auditory notification of the ITMS operator about a vehicle found in wanted vehicle databases.
- Visual and auditory notification of the ITMS operator about the presence/absence of queues of vehicles at entry points to road BCPs.
- Generating reporting documentation (for BCPs, regional customs offices, violations of customs formalities during customs control, by time, by countries of vehicle registration, etc.) in *.pdf, *.xlsx, and other formats.
- Control over the movement of vehicles in controlled territories (control over the passage of a vehicle through control procedures at the road BCPs), namely:
  - Entry into the territory.
  - Border control.
  - Weighting.
  - Scanning
  - Customs control and clearance.
  - Inspection of vehicles in enhanced inspection areas.
  - Exit from the territory, etc.
- Backup and restoration of the system at the road BCPs level and Monitoring Center of the Customs.
- Availability of a data exchange system at the road BCP (IPCT) and the main data exchange system at the central part (core) of the system capable of processing no less than 2000 IPCT.
- Maintaining the archive of technical documentation.
- Generating a database obtained from integrated systems regarding each vehicle, namely:
  - Date and time of vehicle entry into the BCP.
  - Name of the BCP and corresponding customs authority.
  - Photo of the vehicle cabin with the license plate.
  - Photo of the front license plate of the vehicle.
  - Photo of the trailer/semi-trailer or rear part of the vehicle with the license plate.
  - Photo of the rear license plate of the vehicle.
  - Recognized (in text format) front and rear vehicle license plates.
  - Country of vehicle registration.
  - Information from the vehicle weighing system.
  - Unique number of the weighing complex where the vehicle was weighed.
  - Recognized (in textual form) the front license plates of the vehicle at the weighing complex.
  - Vehicle movement algorithm, indicating how decisions regarding vehicle movement were made (automatic, "manual" control).
  - An image of the vehicle was processed by the Scanning System (SS) operator, which was inspected using an SS.
  - A unique number of the SS is used for vehicle inspection.
  - Recognized (in textual form) the front license plates of the vehicle upon exit from the SS area.
  - Vehicle lane – "red corridor", "green corridor", for buses, neutral (diplomatic).

- Login of the customs official who processed the vehicle registration.
- Login of the State Border Guard Service official who processed the vehicle registration.
- Official identification number of the customs officer and/or State Border Guard Service official in case manual barrier opening was performed using a card.
- Date and time of vehicle departure from the territory of BCP.
- Recognized (in textual format) the front and rear license plates of the vehicle upon exit from the territory of BCP.
- Direction (into Ukraine, out of Ukraine).
- Duration of stay within the territory of BCP.
- Performing an analysis of the passage of customs procedures at all stages in BCPs and based on the analysis results, allowing, or prohibiting the exit of vehicles from the customs control zone through software-controlled barriers.
- Formation of an operational response protocol for the operator, based on alarms received from ITMS installed in the BCP area, with the ability to print it out.
- The search in the database of the ITMS according to defined criteria.
- The export of data from the ITMS database into files in *.xlsx (*.xlsx), *.pdf, *.xml, etc., formats.

The software of the ITMS system must meet the following requirements:

- Providing technical support for the operability of the software throughout the warranty period of not less than 5 years.
- The free provision of new software (SW) versions should be carried out as they are released to ensure the full functionality of the SW throughout the warranty period.
- Installation of SW using an MSI file/exe file.
- The setup and subsequent administration of the system should be conducted from a centralized administrator's location.
- An option to generate and store error reports in the SW must be provided.
- Support for multiple user categories (for example: administrator, security, operator, etc.).
- The presence of multi-level password protection to restrict access to video information.
- The presence of user access restriction to software settings with the ability to input a password of up to 16 characters.
- The presence of user account management support.
- Monitoring of actions performed by system users.
- Registration of all user actions in the system (logging).
- The ITMS must automatically erase all recorded video footage from the server after six months to comply with data privacy regulations and manage storage capacity. The vendor must ensure secure and reliable data deletion processes and provide thorough documentation for compliance verification.
- The software should provide the option to receive and process information from the following systems:
  - Reading vehicle license plates.
  - Access control and management.
  - Weighing vehicles.
  - Scanning systems.
  - other systems (if necessary).

  Availability of both individual and group settings for users or objects. See Annex 1 for an example list of user roles and functions.

Within the system, there should be a configured role-based user model with the ability to differentiate access rights and the capability to create an unlimited number of users for each role.

- The system should be supplied with flexible and dynamic access management tools based on Role-Based Access Control (RBAC).
- The specific BCPs, CI, or informational resources to be integrated into the pilot project will be determined by the Customer.

A localized interface (Ukrainian and/or English language) and all documentation in the Ukrainian language.

- The software should function under the management of MS Windows or *nix-like operating systems.
- Support for saving data in non-expired relational databases supported by the respective manufacturer.
- Compatibility with antivirus protection systems.

The interface should be in the form of a multi-level interactive map (country, region, road BCP [controlled territory]), on which alarms generated according to specified parameters for the CIIP operator should be displayed. In road BCP (Controlled Territory) where CIIP integration components are installed, and if they are present, they should be displayed on the map at the locations of the road BCP.

- At the first level, there should be a map of Ukraine divided into zones of activity of the Customs with road BCPs depicted on it as circles.
- For the detailed interventions viewing, when clicking on the map in the respective region (customs activity zone), a second level of interactive map should open with the locations of the corresponding BCPs represented as circles; upon clicking on the map on the respective BCP (circle), a third level of interactive map should open, showing the controlled territory, namely the BCP layout, with equipment systems installed at the BCPs (video cameras, weighing complexes, scanning systems, etc.) marked on it.
- On the third level, the operator should be able to view real-time video footage from each of the installed video cameras, as well as access their video archives. Additionally, they should have the ability to work with the ITMS database in the form of a table, which must contain the following data:
  - Date and time of vehicle entry into the BCP.
  - Name of the BCP and corresponding customs authority.
  - Photo of the vehicle cabin with the license plate.
  - Photo of the front license plate of the vehicle.
  - Photo of the trailer/semi-trailer or rear part of the vehicle with the license plate.
  - Photo of the rear license plate of the vehicle.

- Recognized (in text format) front and rear vehicle license plates.

  - Country of vehicle registration.

- Type of movement according to the selected lane and defined algorithm.

  - Information from the vehicle weighing system.
  - The unique identifier of the weighing complex where the vehicle was weighed.
- Recognized (in textual form) front vehicle license plate at the weighing complex.
- The results of scanning the vehicle registration documents, including images of the documents processed by the operator, which have undergone inspection using the scanning system.
- The unique SS identification number used for vehicle inspections.

- The recognized (in textual form) front license plates of vehicles at the exit from the scanning system area.
- Traffic lane: cargo direction (empty, hazardous, special status goods) passenger direction: red, green, bus, diplomatic.
- The service identification number of the official of the Customs Authority/State Border Guard Service who processed the vehicle registration.
- Official identification number of the customs officer and/or State Border Guard Service official in case manual barrier opening was performed using a card.
- Date and time of vehicle departure from the territory of BCP.
- Recognized (in textual format) the front and rear license plates of the vehicle upon exit from the territory of BCP.
- Direction (into Ukraine, out of Ukraine).
- Duration of stay within the territory of BCP.

Also, the operator must have access to and display information about the following events in the BCP:

- The presence or absence of queues at the entrances to the BCP from both the Ukrainian side and the side of the neighboring state.
- The functionality of the equipment of the ITMS component systems (video cameras, servers, network storage).
- In case there is no information in the data table about the stages of customs formal procedures in the BCP, such as weighing and scanning, it should be displayed in the table in red.
- Information about a vehicle found in the search databases (in the form of visual and auditory notification with a photo of the found vehicle and information about the corresponding database).
- The ability to generate and view databases of found vehicles in the search databases and the ability to search them by vehicle number.
- Visual and auditory informing of the ITMS operator about vehicles that have moved more than once in the last 24 hours (analysis should be carried out only in case of movement from the territory of an adjacent state to the territory of Ukraine).
- Visual and auditory informing of the ITMS operator about the passage of vehicles through the gates for vehicle turnaround at the BCP.
- Visual and auditory informing of the ITMS operator about the entry of vehicles into the deep inspection area.

It is necessary to provide the ability to install ITMS software on the workstations of Customs and State Border Guard Service officials who perform customs/passport clearance at the BCPs, which should ensure:

- Visual and auditory notification (with a photo of the found vehicle) about vehicles found in the wanted databases.
- Visual and auditory notification (with a photo of the found vehicle) about vehicles that have moved more than once in the last 24 hours (analysis should be conducted only in the case of movement from the territory of the neighboring state to the territory of Ukraine).
- Real-time video footage of vehicles when the vehicle was in front of the barrier at the entry point to the area where control procedures are carried out, namely: video footage of the vehicle cabin with the vehicle license plate, which should be visible.
- The IPCT software, in an appropriate number of software modules, should have the following operational capabilities (not exclusively, but including):

It should be a flexible, scalable, reliable, and powerful central management system, providing a single, simple, and effective centralized management of the security system and performing functions such as adding a control device, real-time viewing, video file storage, and playback, alarm signal integration, access control, attendance time tracking, person identification, etc.

It should meet the requirements for full operation and may include the following subsystems:

- Security, alarm, and perimeter signaling systems at both hardware and software levels.
- Security and technological video monitoring system.
- License plate recognition system.
- Access control and electronic visitor request processing system.
- Facial and body recognition system.
- Diagnostic system for all equipment within the system and viewing network details between device nodes in the topology, port information, and connection path verification.

Main functions:

- Support for the open ONVIF standard.
- Compatibility with most major IP camera brands supporting ONVIF.
- Support for third-party patented protocols from leading camera manufacturers, with regular updates.
- Support for OpenSDK, allowing users to develop add-ons on the web client.
- Integration support with third-party security systems.
- Rapid streaming and playback from any NVR/DVR/CVRs.
- Support for advanced user management, including Client Control, Web Client, and Mobile APP.
- Support for alarm and event management (video analytics, POS, etc.).
- Support for E-map, the load management center.
- Support the equipment status monitoring.
- Configuration of module placement on the control panel.
- Hardware decoding.
- Reception of alarm signals.
- System login with domain user account.
- Account lockout after 5 failed password attempts.
- Intelligent window division based on the number of cameras during viewing or playback.
- Map management support.
- Alarm and event signals support.
- Support for decoders, keyboard management, intelligent video wall control, PC-based wall management, online/video/archive/alarm screen control, inter-screen roaming, schedule viewing, etc.
- Support for automatic license plate recognition camera management.
- Support for UVSS (Under Vehicle Monitoring System) camera management.

Real-time viewing and playback:

- Ability for simultaneous viewing of up to 256 channels.
- Ability to correct the fisheye effect.
- Ability to control PTZ visualization.
- Support for decoding streams from high-definition cameras, particularly panoramic cameras.

- Frame-by-frame playback capability.
- Digital zooming during viewing and playback of video.
- Reverse video playback.
- Event-based playback, including motion detection, intrusion detection, and line-crossing analysis.
- Ability to add tags for marking important video footage.

Recording and storage of visual tracking:

- Support for recording schedules for continuous recording, event recording, and command recording.
- The ability to store video on encoding devices, hybrid SANs, and cloud storage servers.
- Ability to provide primary and auxiliary storage.
- Ability to enable video copying.
- Ability to store alarm images on video recorders, hybrid SANs, and cloud storage servers.
- Ability to support video footage search related to VCA events.

Facial and body recognition:

- Ability to display information about recognized individuals in real-time mode.
- Ability to search history records of recognized individuals, including search in captured images, matching individuals, feature-based search, and frequent appearances search.

Intelligent analysis:

- Ability to support resource group establishment and data analysis across different groups.
- Ability to support intelligent analytical reports, including people counting, crowd density analysis, queue analysis, path analysis, individual feature analysis, temperature analysis, and vehicle analysis.
- Ability to display the number of people in defined areas of the facility in real-time mode.

Network management:

- Ability to manage network transmission devices such as switches, display network connection, and hierarchical relationships of controlled resources through topology.
- Ability to view network metrics between nodes in the topology, such as outbound and inbound speeds, port information, etc.

Detailed Specifications: Video Monitoring & Analyzing Subsystem Requirements (hardware)

I. The system should be built on a modular principle. The basic modules of the system are:
   - software and hardware complex for video analytics and centralized database management.
   - software and hardware means for implementing the business logic of the functionality application, which provides the functionality of automated workplaces (a set of specific functions, based on the tasks and responsibilities of the specialist role when working with the system).
   - Video monitoring tools.

II. The system should be built using the "Private Cloud" technology. Within the private cloud, a "Platform as a Service" (PaaS) model should be implemented - a model where consumers are

provided with the ability to utilize cloud infrastructure for hosting base software to subsequently add new or existing applications (proprietary, custom-developed, or purchased applications).

III. The system should consist of the following elements.

Item	Detailed Specifications
The Video Storage Server for building a cloud platform at SCSU servers, must have technical and other characteristics following the following requirements (not less than):	▪ secure communication with the control processor using SSL, SSH certificates, and the ability to integrate with LDAP or Active Directory of the Customer for access authorization. ▪ the ability to communicate with the control processor via a paid network port of the server; the ability to directly connect a keyboard, mouse, and monitor directly to the server. ▪ the ability to remotely connect a keyboard, display, and mouse (remote KVM access), which are defined by the computer as local; ▪ all required server management functionality must be provided by a management processor built into the server with management software with a free perpetual license. ▪ the delivery set must also include separate software with a 12-month license in the form of a virtual machine for installation in virtual environments such as VMware, Microsoft Hyper-V, and KVM while providing the same functionality as the built-in software, as well as: centralized deployment, monitoring, management, server life cycle management, as well as support for physical and virtual infrastructure from a single window in a web browser as a web page;.
A Hard Disk Drive for storing information must have technical and other characteristics per the following requirements (not less than):	▪ Storage capacity: at least 6 TB. ▪ Compatibility (not less than): MAC OS, Windows, Linux. ▪ Hard drive type: internal. ▪ Technology: HDD. ▪ Form factor: 3.5 ". ▪ Interface: SATA III. ▪ Spindle rotation speed (not less than): 7200 RPM. ▪ Buffer size (not less than): 256 MB. ▪ Average waiting time (not less than): 4.16 ms. ▪ Data transfer rate (not less than): 226 MB/s. ▪ Maximum power consumption (not less than): 11.67 W. ▪ Mean time to failure (not less than): 2 million hours.
The server for operating cloud platform management	▪ Server for installation in a 19” standard cabinet. ▪ height not more than 2U. ▪ at least two processors, up to 28 cores per processor. ▪ memory controllers are not worse than the HBA type.

must have technical and other characteristics following the following requirements (not less than):	▪ Memory not worse than 24 DDR5 DIMM slots, with RDIMM / LRDIMM support, speed up to 5600 MT / s, 3TB maximum up to 12 NVDIMM, 192 GB maximum. ▪ mandatory provision of single and multi-bit memory error detection and single-bit error correction (ECC). ▪ regular check reading of memory blocks to prevent the accumulation of corrected errors. ▪ Mandatory support for graphics processing units (GPUs) with CUDA architecture. ▪ Support for multi-GPU technology is recommended to increase memory capacity and improve performance for complex visual computing. ▪ Hard disk type (required): SAS disks of Enterprise Performance level with DWPD not less than 3. ▪ maximum hard disk capacity (not less than): 6 TB. ▪ storage controller (required): hardware 12G SAS RAID controller with nonvolatile cache memory of at least 4 GB. ▪ RAID level support (required): 0, 1, 5, 6, 50. ▪ Support for RAID levels (recommended): 10, 60. ▪ support for at least 24 internal SAS HDD and SAS/SATA SSD disks; support for hot-swapping disks, online migration, and array expansion; -system power supply (not worse): 1+1, 220V power supplies with a capacity of at least 1200 W (with hot-swap support) with power cables included. Power factor not worse than 0.95 at 50% load;-Availability of a separate module with a cryptographic signature TPM 2.0, TCG, FIPS140-2, CC EAL4+;-video subsystem (not worse): integrated 2D graphics with hardware acceleration, the maximum resolution of which is not lower than 1920x1200 16bpp @ 60Hz;-Kit for cabinet mounting, availability of telescopic rails;-Availability of ports (not worse): 4 x 1GE; 2 x USB 2.0, USB 3.0, VGA. ▪ Network adapters (required): support for converged network adapters for organizing at least 4 Fiber Channels, NVMe-over-FC connection channels, as well as at least 16 Ethernet channels. Supports logical partitioning of up to 256 virtual NICs and HBAs supporting Ethernet, iSCSI, FC, FCoE, NVMe-over-FC, VXLAN, and NVGRE. Supports network factory consolidation with a single management center; -Support for network adapters with 10 Gbps SFP+ Ethernet ports; -The server must have official manufacturer support and certification for Microsoft Windows Server of the latest release at the time of system installation. ▪ The server must be officially supported by the manufacturer and certified for the latest version of

	VMware vSphere at the time of system installation. ▪ The server must support Linux operating systems such as RHEL, SUSE, and SLES;-The server must be able to operate in the same landscape with blade servers using common Ethernet and Fiber Channel switching modules;-Mandatory availability of a validated design for building server-network-storage platforms with at least 3 global storage vendors, such as IBM, Hitachi, Pure Storage, NetApp, DELL EMC, HPE. ▪ A processor with a separate network port with a speed of at least 1 GB/s and management software (free of charge) built into the server with the following functions: a. gathering statistics from the server; b. monitoring of its power supply and temperature, and the status of server components both before and after loading the operating system (without the need to install agents in the operating system). c. access to the graphical console of the server through a browser and to the text console through a terminal emulator. d. loading the server for configuration, deployment, and installation of a compatible operating system without installing additional media on the server. e. communication with the support site for automatic notifications about the status, configuration change, and failure. f. secure communication with the control processor using SSL, and SSH certificates and the possibility of integration with the Customer's LDAP or Active Directory for access authorization. g. possibility of communication with the control processor through the paid network port of the server. h. possibility of directly connecting a keyboard, mouse, and monitor directly to the server. i. the ability to remotely connect a keyboard, display, and mouse type manipulator (remote KVM access), which are determined by the computer as local. j. all required server management functionality must work through the server's built-in management processor with management software with a free perpetual license. ▪ The delivery set should also include separate software with a license for 12 months in the form of a virtual machine for installation in virtual environments such as VMware, Microsoft Hyper-V, and KVM while providing the same functionality as the embedded software, as well as: centralized deployment, monitoring, management,

	maintenance of the life cycle of servers, as well as support of physical and virtual infrastructure from a single window in a web browser in the form of a web page; ▪ The system must include a redundant power supply to ensure continuous operation in case of a primary power source failure
A 24-port cloud commutator must have technical and other characteristics according to the following requirements (not less than):	▪ PU (no less than): Frequency 800 MHz. ▪ ROM / RAM (not worse): 512Mb. ▪ Ethernet ports (Uplink) (no less than): 2x SFP / SFP +. ▪ Ethernet ports (Downlink) (not worse): 24x RJ45 (10M / 100M / 1000M). ▪ availability of voltage monitoring function. ▪ VLAN (not worse): IEEE 802.1Q. ▪ recommended support for data stacking technologies through individual or network ports. ▪ availability of port mirroring function. ▪ management (not worse): L2. ▪ availability of temperature monitoring on the board. ▪ the presence of a processor radiator. ▪ the presence of heat sinks on the chip. ▪ MAC table size (not worse): 16K. ▪ flow management support. ▪ power supply (not worse): DC 9.6 - 60V, the system must include a redundant power supply to ensure continuous operation in case of a primary power source failure ▪ power consumption (not worse): 24W. ▪ support for two DC power supplies. ▪ support for connecting expansion modules with Ethernet ports. ▪ working temperature (not worse): -40º to + 60ºC. ▪ humidity (no less than): 10% ~ 90% RH. ▪ Support for such functionality (no less than) — IEEE 802.1, 802.3 standard, NTP, UDLD, CDP, LLDP, unicast MAC filter, PAgP, LACP VTPv2, VTPv3, EtherChannel, Q-in-Q tunneling, voice VLAN, PVST+, MSTP, and RSTP, IGMPv1, v2, v3 snooping, IGMP filtering, IGMP querier, WebUI, MIB, SmartPort, SNMP, syslog, DHCP server, SPAN session, RSPAN, FSPAN, Express setup, NETCONF, RESTCONF, Port security, 802.1x, Dynamic Host Configuration Protocol (DHCP) snooping, dynamic ARP inspection, IP source guard, guest VLAN, MAC authentication bypass, 802.1x multidomain authentication, storm control - unicast, multicast, broadcast, SCP, SSH, SNMPv3, TACACS+, RADIUS server/client, MAC address notification, BPDU guard, Access Lists (PACL,VACL,RACL), SUDI 2099 (Secure

	Unique Device identifier), Full Flexible NetFlow (FNF), MACsec-128, FIPS 140-2, Ingress policing, rate limit, egress queuing and shaping, auto QoS, IPv6 host support, SNMP over IPv6, HTTP/HTTP(s) over IPv6, SNMP over IPv6, Syslog over IPv6, DHCPv6 relay source, DHCPv6 bulk lease query (RFC 5460), IPv6 stateless Auto Config SCP/ SSH, Radius, TACACS+, NTP over IPv6, IPv6 VRF aware BGPv6, IPV6 ND cache expire, IPv6 support for TFTP, IPv6 DNS transport, IPv6 QoS, IPv6 FHS RA Guard, IPv6 FHS DHCPv6 Guard, Inter-VLAN routing, Static routing, CIP Ethernet/IP, IEEE 1588 PTP v2 (default and power), PROFINET, Resilient Ethernet Protocol (REP) ring, PROFINET-Media Redundancy Protocol (MRP), REP Preferred, Fast REP, Dying gasp, SCADA protocol classification - GOOSE messaging, MODBUS TCP/IP, YANG, NETCONF, RESTCONF, Layer 2 switching with 1:1 switch Network Address Translation (L2NAT). ▪ Support for SDN technology for corporate or industrial networks, namely the Cisco SD-Access architecture (or equivalent). ▪ The equipment must support at least 1 Virtual Network (VN) and the ability to perform such roles in the SD-Access factory as Fabric Border and Control Plane and Fabric Extended. ▪ The factory Cisco SD-Access controller (or equivalent) must be free and available to download in virtual form for private on-premises deployment in the VMware vSphere (ESXi) virtualization system.
The PoE switch must have technical and other characteristics following the following requirements (not less than):	▪ ROM/RAM (no less than): 128Mb / 16Mb. ▪ Ethernet ports (Uplink) (not worse): 4x SFP (1000M). ▪ Ethernet ports (Downlink) (not worse): 8x RJ45 (100 / 1000M) with PoE support. ▪ COM port (no less than): RJ45. ▪ PoE protocols (not worse): 802.3af / at. ▪ recommended support for data stacking technologies through individual or network ports. ▪ maximum bandwidth (no less than): 12 Gbit / s. ▪ packet forwarding speed (not worse): 17.8 Mpps. ▪ availability of management. ▪ availability of temperature monitoring on the board. ▪ mirroring of ports: incoming/outgoing traffic. ▪ VLAN (not worse): 802.1Q VLAN (up to 4K simultaneous networks). ▪ power supply (not worse): DC 9.6-60V. ▪ consumed power (no less than): 10W.

	▪ support for two DC power supplies. ▪ support for connecting expansion modules with Ethernet ports. ▪ working temperature (not worse): -30ºC ~ + 55ºC. ▪ humidity (no less than): 10% ~ 90% RH. ▪ Support for such functionality (no less than) — IEEE 802.1, 802.3 standard, NTP, UDLD, CDP, LLDP, unicast MAC filter, PAgP, LACP VTPv2, VTPv3, EtherChannel, Q-in-Q tunneling, voice VLAN, PVST+, MSTP, and RSTP, IGMPv1, v2, v3 snooping, IGMP filtering, IGMP querier, WebUI, MIB, SmartPort, SNMP, syslog, DHCP server, SPAN session, RSPAN, FSPAN, Express setup, NETCONF, RESTCONF, Port security, 802.1x, Dynamic Host Configuration Protocol (DHCP) snooping, dynamic ARP inspection, IP source guard, guest VLAN, MAC authentication bypass, 802.1x multidomain authentication, storm control - unicast, multicast, broadcast, SCP, SSH, SNMPv3, TACACS+, RADIUS server/client, MAC address notification, BPDU guard, Access Lists (PACL,VACL,RACL), SUDI 2099 (Secure Unique Device identifier), Full Flexible NetFlow (FNF), MACsec-128, FIPS 140-2, Ingress policing, rate limit, egress queuing and shaping, auto QoS, IPv6 host support, SNMP over IPv6, HTTP/HTTP(s) over IPv6, SNMP over IPv6, Syslog over IPv6, DHCPv6 relay source, DHCPv6 bulk lease query (RFC 5460), IPv6 stateless Auto Config SCP/ SSH, Radius, TACACS+, NTP over IPv6, IPv6 VRF aware BGPv6, IPV6 ND cache expire, IPv6 support for TFTP, IPv6 DNS transport, IPv6 QoS, IPv6 FHS RA Guard, IPv6 FHS DHCPv6 Guard, Inter-VLAN routing, Static routing, CIP Ethernet/IP, IEEE 1588 PTP v2 (default and power), PROFINET, Resilient Ethernet Protocol (REP) ring, PROFINET-Media Redundancy Protocol (MRP), REP Preferred, Fast REP, Dying gasp, SCADA protocol classification - GOOSE messaging, MODBUS TCP/IP, YANG, NETCONF, RESTCONF, Layer 2 switching with 1:1 switch Network Address Translation (L2NAT). ▪ Support for SDN technology for corporate or industrial networks, namely the Cisco SD-Access architecture (or equivalent). ▪ The equipment must support at least 1 Virtual Network (VN) and the ability to perform such roles in the SD-Access factory as Fabric Border and Control Plane and Fabric Extended. ▪ The factory Cisco SD-Access controller (or equivalent) must be free and available to download in virtual form for

	private on-premises deployment in the VMware vSphere (ESXi) virtualization system.
The router must have technical and other characteristics following the following requirements (not less than):	▪ -hardware accelerated RJ-45 GE ports: 18 ▪ -hardware accelerated SFP GE slots: 8. ▪ - hardware accelerated SFP+10 GE:4 slots. ▪ - Volume of internal storage: 1x480 GB SSD (no less than) ▪ - Bandwidth of the firewall (1518/512/64 bytes UDP): 27 / 27 / 11 Gbps ▪ - IPS bandwidth: 5 Gbps. ▪ - IPsec VPN bandwidth: 13 Gbps. ▪ - NGFW (Enterprise Mix) bandwidth: 3.5 Gbps ▪ - Firewall policies: 10000. ▪ -SSL VPN Bandwidth: 2 Gb/s ▪ -SSL VPN simultaneous users: 500. ▪ - power supply (not worse): 100 / 240V. ▪ -consumed power (not worse): 122W. ▪ - working temperature (not worse): 0 ° C . + 40 ° C. ▪ - Support for such functionality (no less than): ▪ -Classic firewall - stateful firewall. ▪ - Network mode: ▪ - L3 firewall, ▪ - L2 firewall, ▪ - virtual firewall context, support for simultaneous operation of virtual contexts in L2 and L3 on one device: ▪ -At least 2 virtual firewalls with dedicated resource control and self-management. ▪ - Support for at least 100 such virtual firewalls. ▪ -The system should allow you to choose the type of operating system according to the functionality between the classic firewall and the next-generation firewall when initializing the device. ▪ -Fault resistance: ▪ - Active/Active, necessarily with synchronization of session states. ▪ - Active/Standby. ▪ -Internet screen with identification functions: ▪ - authentication of users in the active directory (MS AD agent). ▪ - the possibility of forming and implementing an access policy by user groups from different directories (MS AD, multiforest AD, or LDAP). ▪ - the possibility of forming and implementing an access policy for groups of devices. ▪ -Functional principles of building the architecture of the protection of traffic processing devices: ▪ - the architecture should provide for the absence on the

	hardware platforms of traffic processing devices of services that can affect the operation of the main functionality, using resources for computationally burdensome processes, in particular: ▪ - anti-spam (Antispam). ▪ - information leak prevention system (DLP) with restrictions on free distribution. ▪ - WAN traffic optimization services. ▪ - routing protocol OSPF, EIGRP, BGP. ▪ - Remotely Triggered Black Hole (RTBH) for Border Gateway Protocol (BGP) security. ▪ -Non-Stop Forwarding (NSF) in fail-safe mode (HA) when one of the pair's devices fails. ▪ -Services – IPv4, IPv6 and Ethernet: ▪ - static translation of network addresses (Static NAT). ▪ - dynamic translation of network addresses (Dynamic NAT). ▪ - broadcast of port addresses (PAT). ▪ - real-time traffic redirection protocol to caching devices (Cache Engines). ▪ - Layer 2 Tunneling Protocol (L2TP). ▪ -Multicasting: IGMP, PIM-SM, Bidirectional PIM. ▪ -The system should have a built-in ability to create and configure rules using the SNORT language. ▪ -Inspection at the application level: ▪ - inspection of correct operation (IPv4 options; DNS over UDP, HTTP FTP, H.323/H.225). ▪ - GTP inspection when adding the appropriate license. ▪ -Functions of protection against DDoS attacks. ▪ - Detection and classification of network traffic of application-level applications (Application firewall). ▪ -Recognition of at least 4000 applications ▪ -Protection against network attacks with the following functionality: ▪ - stateful DPI at levels 3-7 of the OSI model. ▪ - detection of NSD attempts in real-time. ▪ - real-time prevention of NDS attempts by blocking or terminating unwanted network sessions. ▪ - built-in lifetime IPS signatures. ▪ - countering defense bypass techniques. ▪ - Subscription to Update Signatures (IPS) ▪ -Provision of URL filtering: ▪ - at least 80 categories. ▪ - Categorization of at least 280 million URLs. ▪ - the ability to redirect HTTP (s) traffic to an external multi-level filtering service with automatic load balancing. ▪ - Ensuring protection against malicious software:

	▪ - with the possibility of retrospective analysis, search, and display of distribution paths. ▪ -The system must be able to passively detect endpoints and infrastructure to correlate threats and indicators of compromise (IoC). ▪ -Automated update channel of threat signatures and IPS policies from leading information security intelligence (CSI) centers. ▪ - support for RADIUS, TACACS or TACACS+ protocols, LDAP, Kerberos, and One-Time Password systems. ▪ - support of digital certificates. ▪ - authentication and authorization of users using HTTP, HTTPS, FTP, and SSH v2 protocols. ▪ - SNMP protocol versions 1, 2, 3. ▪ - provision of different levels of access to the device. ▪ - a protocol for collecting aggregated information about IP flows (source and destination IP addresses, TCP/UDP ports) (NetFlow, NSEL). ▪ -The system should be able to be managed using CLI, HTTP, HTTPS, and API. ▪ -The system should be capable of centralized configuration, logging, monitoring, and reporting or in the cloud using an orchestrator. ▪ -The system must include trusted binding technologies to secure supply chains and ensure the integrity of software instances. ▪ - The system should provide the possibility of integration with platforms for sharing/spreading information about malicious software. ▪ -Must support collection of malware information from various sources. ▪ - The system should be able to fully integrate with external vulnerability scanners - at least Qualys, and Nessus. ▪ - The system must have support for exchanging information about security tags (Security-Group Tags) with compatible systems.
The structured cable network must meet the following requirements:	▪ To combine the elements of the cloud platform into a single information network, it is necessary to create a structured cable network (hereinafter referred to as SCN), which must meet the following standards: o utilize a minimum of CAT 6 network cabling o DSTU B A.2.4-40:2009. o DSTU B A.2.4-42: 2009. o TIA/EIA-568 A(B) Commercial Building Telecommunications Cabling "Cabling for

	telecommunications products and services in commercial buildings". o ISO/EIC 11801 "Information technologies. Universal cable network for the customer's buildings and territories". o TIA/EIA-862 Building Automation Systems Cabling Standard for Commercial Buildings. o EN 50173 Information technology – Generic cabling systems. o ISO/IEC TR 14763 Information technology - Implementation and operation of customer premises cabling. o TIA/EIA-942 Telecommunications Infrastructure Standard for Data Centers o BICSI Telecommunication Distribution. Methods Manual. 10th Edition: 2003 o PUE "Rules of electrical installations", o as well as meet the requirements for category 5e cable networks. o SCN must ensure: o a combination of key elements of the cloud platform into a single information network. o reliability and ease of use. o speed of information transfer: 10/100/1000 Mb/s. o the possibility of expanding the system. ▪ The topology of SCN assembly is a "hierarchical star". ▪ The number and characteristics of the component elements for the deployment of SCN must be determined by the Contractor at the stage of the inspection of the object together with the Customer. ▪ All SCN components must be manufactured by well-known manufacturers in compliance with international quality certificates (ISO 9001, ISO 9002). For the installation (mounting) of the SCN, a symmetrical copper cable of the "twisted pair" type should be used, designed for data transmission using Gigabit Ethernet (1000BASE-T) category 5e technology. ▪ SCN should be divided into structural subsystems: a set of copper cables, switching panels, organizers, and cable connectors. ▪ The cables of the power supply network and the low-current system must be laid in separate cable channels. In workplaces and on all evacuation routes (corridors, transitions), it is mandatory to use cables whose sheath does not support the combustion process does not contain halogens, and does not emit poisonous gases in case of fire.

	▪ Installation of a structured cable network must be carried out per the requirements of current standards by qualified personnel. For the passage through the walls, collateral plastic pipes should be provided, sufficient for laying the necessary number of cables, taking into account the technological reserve and meeting the requirements of the standards for the level of cable filling. In the process of preparing the cable ducts for laying the cable, the absence of sharp corners and burrs on the inner surfaces should be checked. ▪ SCN testing: ○ after carrying out work on the installation of SCN, all unshielded twisted pair cables are checked for compliance with category 5e cable networks for internal office premises. ○ testing is performed for each data transmission channel. ▪
Telecommunication cabinet 19"the set must have technical and other characteristics per the following requirements (not worse):	▪ front door: with turning handle, lock, and tempered glass. ▪ rear door: all-metal with "gill" type perforation and lock. ▪ side walls: removable with a lock. ▪ coating: powder coating. ▪ cabinet design: collapsible. ▪ class of protection against external factors: not less than IP 20. ▪ the supporting structure is made of 1.5-2.0 mm steel (not less than). ▪ the ability to adjust the distance between rivers by depth.
The uninterruptible power supply must have technical and other characteristics per the following requirements (not less than):	▪ number of sockets (not worse): 6 x IEC 320 C13 (battery backup power); 4 x IEC 320 C19 (battery backup). ▪ output power (not worse): 5000 VA / 4500 W. ▪ input voltage range when working from the mains (not less than): 160 - 275 V. ▪ working time at full load (not worse): 4 min (4500 W). ▪ working time at half load (not worse): 11.8 min (2250 W). ▪ rechargeable battery: built-in. ▪ impulse protection (not less than): 480 J. ▪ type of battery used (not less than): sealed lead-acid battery with thickened electrolyte: protection against leaks. ▪ type of architecture (not less than): continuous operation. ▪ availability of an LCD. ▪ battery charging time (not less than): 1.5 hours. ▪ output voltage form: pure sinusoid.

A set of rechargeable batteries for the uninterruptible power supply must have technical and other characteristics per the following requirements (not less than):	▪ battery output voltage (not worse): 192 V. ▪ type of batteries: lead-acid battery. ▪ compatibility with the uninterruptible power supply, the requirements for which are specified above; ▪ expected battery life (not less than): 3-5 years. ▪ working temperature (not worse): 0 - 40 ° C. ▪ working range of relative humidity (not worse): 0 - 95% (without condensation).
The monitoring video camera for the server room must have technical and other characteristics per the following requirements (not less than):	▪ the lens is not less than 1 / 3 "Progressive Scan CMOS. ▪ maximum resolution (not less than): 2560 x 1440. ▪ minimum sensitivity (not less than): 0.01Lux @ (F1.2, AGC on), 0.018Lux @ (F1.6, AGC on), 0 Lux with IR. ▪ shutter speed (not less than): 1/3 s-1 / 100,000s. ▪ support for slow shutter speed. ▪ day/night mode (not less than): IR filter (ICR). ▪ axis adjustment (not less than): rotation: 0 ° ~ 355 °; tilt: 0 ° ~ 75 °; rotation: 0 ° ~ 355 °. ▪ illumination range (not worse): 30 m. ▪ focal length (not less than): 2.8-12 mm. ▪ lens mount: F14. ▪ aperture (not less than): F1.6. ▪ viewing angles (not less than): H: 98 ° ~ 28 °, V: 51 ° ~ 16 °, D: 115 ° ~ 32 °. ▪ automatic focus control. ▪ video compression (not exclusively but including): / H.265/ H.264 / MJPEG. ▪ number of streams (not worse): 3 streams. ▪ support for resolutions (not exclusively but including): 4M (2688x1520) / 3M (2304x1296) / 1080P (1920x1080) /1.3M (1280x960) / 720P (1280x720) / D1 (704x576 / 704x480) / VGA (640x480) / CIF (352x288 / 352x240). ▪ frame rate (not exclusively but including): (mainstream) 2688 x 1520, 2304 x 1296, 1920 x 1080 - 25 k / s; Add. stream) 640 x 480, 640 x 360, 320 x 240 - 25 k / s; Addendum 2 stream: 1280 x 720, 640 x 360, 352 x 288 - 25 k / s. ▪ video bitrate (not worse): 32 Kbit / s - 16 Mbit / s. ▪ noise suppression (DNR) (not worse): 3D DNR. ▪ BLC support. ▪ WDR (not worse): 120 db. ▪ ROI (not less than): 1 fixed area for the mainstream and sub-streams.

	▪ image settings Rotation mode, saturation, brightness, contrast, and sharpness are adjusted by client software or web browser. ▪ audio compression (not exclusively, but including): G.711 / G.722.1 / G.726 / MP2L2 / PCM ▪ audio bitrate (not exclusively but including): 64Kbit / s (G.711) / 16Kbit / s (G.722.1) / 16Kbit / s (G.726) / 32-160Kbit / s (MP2L2). ▪ Ethernet (not worse): RJ45 10M / 100M. o network protocols (not exclusively, but including): TCP / IP, ICMP, HTTP, HTTPS, FTP, DHCP, DNS, DDNS, RTP, RTSP, RTCP, PPPoE, NTP, UPnP ™, SMTP, SNMP, IGMP, 802.1X, QoS, IPv6, Bonjour; compatibility (not exclusively, but including): ONVIF (PROFILE S, PROFILE G), ISAPI; o storage method (not exclusively, but including): NAS (NFS, SMB / CIFS), ANR, Micro SD. o - browser support (not exclusively, but including): IE8 +, Chrome 31.0-44, Firefox 30.0-51, Safari 8.0+. o mobile platforms (not less than): iOS, Android. o users/levels (not worse): up to 32 users; 3 levels: administrator, operator, and user. o video interfaces (not less than): 1Vp-p (75 Ohm / BNC). o audio interfaces (not less than): 1 input / 1 output. o alarm interfaces (not less than): 1 in / 1 out. o network interfaces (not less than): 1 RJ-45 (10M / 100M). o local memory (not less than): micro-SD up to 128GB. o the presence of a reset button. o alarm triggers (not exclusively, but including): motion detection, scene change, network disconnection, IP address conflict, illegal access, storage error. o Smart functions (not exclusively but including): line crossing; invasion of the region; identification of persons. o power supply (not less than): DC 12V ± 25%. o PoE (not worse): PoE (802.3af) (Class 3). o power consumption (not worse): DC 12V: 0.8 A, 10 W; PoE: (802.3af, 37 V-57 V), 0.35A - 0.2A, max. 12 W. o working temperature (not worse): -30 ° C - + 60 ° C. o humidity: <95%. o degree of protection (not less than): IP67, IK10, TVS 2000V.

Detailed Specifications: Operators' Working Station Requirements

Item	Detailed Specifications
Type operator workplace PC 1 must have technical and other characteristics per the following requirements (not less than):	▪ the processor is not less than Core i7-9700F. ▪ RAM not less than 16 GB. ▪ HDD is not less than 2 TB. ▪ SSD is not worse than 240 GB. ▪ video card not less than GTX1050Ti. ▪ the operating system is not less than Windows 11Pro. ▪ PCs must be equipped with endpoint protection and endpoint detection and response (EDR) software to safeguard against cybersecurity threats.
Monitor for operator workplace type 1 must have technical and other characteristics per the following requirements (not less than):	▪ screen type: TFT-LED backlight. ▪ screen size: 24”. ▪ pixel size: no more than 0.3 x 0.3 mm. ▪ screen resolution: not worse than 1920x1080. ▪ brightness: at least 250 cd/m2. ▪ contrast: not worse than 1000:1. ▪ response time: no more than 5 ms. ▪ viewing angle: not less than than 170/160. ▪ interfaces (not less than): HDMI, VGA.
Type 2 operator workplace PC must have technical and other characteristics per the following requirements (not less than):	▪ the frequency of the processor is not worse: 2 GHz. ▪ RAM is not less than 4 GB. ▪ External ports: 1xDC-in Power Connector 1xDisplayPort 1xHDMI 2.0 1xLAN (RJ45) port(s) 1xUSB3.0 1xAudio jack(s) ▪ Wireless communications: Wi-Fi 802.11ac, BT 4.0. ▪ SSD is not worse than 128 GB. ▪ the video card is not less than integrated. ▪ the operating system is not less than Windows 11Pro. ▪ PCs must be equipped with endpoint protection and endpoint detection and response (EDR) software to safeguard against cybersecurity threats.
Type 2 operator workstation monitor must have technical and other characteristics per the following requirements (not less than):	▪ screen type: TN with WLED backlight. ▪ screen size: 21.5”. ▪ screen resolution: not worse than 1920x1080. ▪ brightness: at least 200 cd/m2. ▪ contrast: not worse than 600:1. ▪ response time: no more than 5 ms. ▪ interfaces (not less than): HDMI, VGA.
The keyboard +	▪ interface: USB adapter 2.4 GHz.

mouse set must have technical and other characteristics per the following requirements (not less than):	▪ moisture-proof keyboard. ▪ color: black. ▪
Type 2 uninterruptible power supply	▪ must have technical and other characteristics per the following requirements (not less than): ▪ number of sockets (not worse): 2. ▪ output power (not worse): 800 VA / 480 W. ▪ input voltage range when working from the mains (not less than): 155-275 V. ▪ working time at half load (not less than): 10 minutes. ▪ working time at full load (not less than): 5 min. ▪ type of architecture (not less than): line-interactive (line-interactive). ▪ rechargeable battery: built-in. ▪ the type of battery used (not less than): sealed maintenance-free lead-acid battery. ▪ output voltage form: approximated sinusoid.
Network filter must have technical and other characteristics per the following requirements (not less than):	▪ number of sockets (not worse): 6. ▪ maximum load current (not worse): 10 A. ▪ cable length (not worse): 2 m. ▪ voltage (not worse): 220 V, 50 Hz. ▪ maximum load (not less than): 2200 W. ▪ automatic fuse, max. (not less than): 10 A. ▪ cable cross-section (not less than): 3x1.0 mm. ▪ type: network filter. ▪ filter connection type: for connection to UPS (connector C14). ▪ presence of a switch. ▪ availability of grounding.

Detailed Specifications: Access Control and Management Subsystem Requirements

Item	Detailed Specifications
ACS Controller with two doors must have	• processor (not less than): 32-bit high-speed processor. • number of doors: 2. • communication interface: TCP / IP.

technical and other characteristics per the following requirements (not less than):	• connection interface (not less than): RS-485, Wiegand. • memory (not worse): maps: 100,000; events: 300,000. • status indication (not less than): power supply status, communication status, working status. • wall reader (not less than): via Wiegand (4 readers) or RS485 (up to 4 readers). • input interfaces (not less than): 13 (2 - door sensors, 4 - alarms, 4 - input, 2 - exit buttons, 1 - unauthorized access). • output interfaces (not less than): 2 relay outputs, 4 - alarms. • power consumption ≤100 W. • working temperature (not less than): -20 ° C - +65 ° C.
The battery must have technical and other characteristics per the following requirements (not less than):	• type (not less than): AGM technology. • capacity (not less than): 7Ah. • voltage (not less than): 12V.
Terminal with face and fingerprint recognition function must have technical and other characteristics per the following requirements (not less than):	• operating system: Linux. • camera (not less than): two 2MP each. • a memory of maps and events (not worse): 6,000 maps, 50,000 events. • finger memory (not worse): 5000 fingerprints. • a memory of persons (not worse): 6000 persons. • presence of fingerprint comparison mode. • card reading delay (not less than): <1 s. • delay in reading faces (not less than): <0.2 s. • card type: Mifare. • modes of operation: recognition of persons. • reading distance (not less than): 3 m. • the communication interface (not less than): 1x RJ45 (10M/100M). • input interfaces (not less than): 1x USB, 1x RS-485, 2x alarm input. • output interfaces (not less than): 1x lock, 1x door sensor, 1x exit button, 1x alarm output. • display (not less than): 7-inch touch screen. • power supply (not worse): DC 12V / 2A, 24 W. • working temperature (not less than): from -30 to +60 ° C. • humidity (not less than): from 0 to 90%. • degree of protection (not less than): IP65. • availability of anti-sabotage function.
The exit button for	• device type: exit button.

the server room must have technical and other characteristics per the following requirements (not less than):	• dimensions (no more): 83x32x25mm. • material: stainless steel. • nominal current (not less than): DC12V. • output interfaces (not less than): NO / COM.
Electromagnetic lock with a bar must have technical and other characteristics per the following requirements (not less than):	• device type: electromagnetic lock. • place of installation: premises. • installation type: overhead. • holding power (not less than): 280 kg. • the presence of a door status sensor. • indication: light. • supply voltage/power source: DC 12V / DC 24V. • consumption current (not worse): 500/250 mA. • material (not less than): anodized aluminum (lock) | zinc (bar). • working temperature (not less than): -10 ~ +55 ° C.
Puller must have technical and other characteristics per the following requirements (not less than):	• device type: door closer. • door weight (not worse): 120 kg. • door width: maximum 950-1400 mm. • type of lever: knee. • door opening angle (not worse): from 80 ° to 180 °. • the possibility of adjusting work modes. • color: silver. • working temperature (not less than): from -30° C to +50° C.
Magnetic contact detectors must have standard technical and other characteristics according to the purpose	n/a
Terminal for working with fingerprints must have technical and other characteristics per the following requirements (not	• device type: fingerprint input device. • the communication interface (not less than): USB 2.0. • availability of state indication. • output interfaces (not less than): USB 2.0. • power supply (not worse): 5 VDC, 200mA. • working temperature (not worse): -30 ° C to + 70 ° C. • size (no more): 100mm x 48mm x 35mm.

less than):	• color: black.
Terminal for working with cards must have technical and other characteristics per the following requirements (not less than):	• device type: USB card input device. • communication interface: USB 2.0. • frequency response: 13.56MHz and 125KHz. • availability of state indication. • output interfaces: USB. • power supply: USB. • power consumption (not worse): 200mA. • working temperature (not less than): -20 ° C ~ +65 ° C. • size (no more): 117mm x 67.5mm x 14.3mm. • color: black.
Installation kit - the type and dimensions of the installation kit are specified at the stage of the inspection of the ACS installation facilities, and preliminarily consists of the following parts:	• set of connectors: 1 set. • a set of consumables (screws, bolts, self-tapping screws, dowels, drills, etc.).

Detailed Specifications: Video Monitoring Nodes and Access Requirements

○ **Item**	**Detailed Specifications**
Video camera with license plate recognition type 1 must have technical and other characteristics per the following requirements (not	• lens (not less than): 1 / 2.8" Progressive Scan CMOS. • minimum sensitivity (not less than): Color: 0.002Lux@ (F1.2, AGC ON), B/W: 0.002Lux@ (F1.2, AGC ON). • shutter speed (not less than): 1/30 - 1/100,000 s. • type of illumination (not less than): LED. • lens type: motorized. • focal length (not less than): 3.1 - 9 mm. • aperture (not less than): F1.2. • focus control (not worse): focusing with one touch. • video compression (not worse): H.265, H.264.

less than):	• maximum resolution (not less than): 1920 x 1200. • frame rate (mainstream) (not worse): 25 k / s (1920 x 1200). • video bitrate (not worse): 32 kbit / s - 16 Mbit / s. • support for gain control (AGC). • support for noise suppression (DNR) 3D. • image adjustment support. • network protocols (not exclusively, but including): TCP / IP, HTTP, DHCP, DNS, RTP, RTSP, NTP, FTP for photos. • ANPR support. • LED control (not less than): support for automatic lighting control/time control of LEDs. • image format (not worse): JPEG with adjusted quality. • car color recognition (not exclusively, but including): red, yellow (including orange), green, blue, purple, brown, white, gray (including silver), black. • recognition of the car brand (not exclusively, but including): Hyundai, Toyota, Kia, Honda, Volkswagen, Benz, Nissan, Ford, ISUZU, BMW, Chevrolet, Mitsubishi, Renault, Opel, Suzuki, Skoda, Daewoo, Audi, Mazda, Hino, Peugeot, Ssang Yong, Citroen, Fiat, Scania, MAN, Volvo, Lexus, Seat, Land Rover, Daihatsu, UD Trucks, Subaru, IVECO, MINI, Jeep, Porsche, Chery, Dodge, Chrysler, Acura, Alfa Romeo, Great Wall, Infiniti, Smart, SAIC Maxus, JAC, Jaguar, GMC, Lincoln, JMC, SAAB, FAW, Yutong, Mercury, Joylong, Geely, Cadillac, Jinbei, Ankai, Haima, Foton, King Long, Dongfeng, Emgrand ; • ANPR-supported country/region (not exclusively but including): Turkey, Croatia, Slovakia, Czech Republic, Bulgaria, Macedonia, Hungary, Greece, Poland, France, Netherlands, Switzerland, Spain, United Kingdom, Ireland, Germany, Italy, Austria, Israel, Ukraine, CIS countries. • ANPR recognition accuracy (under recommended installation and lighting conditions) (not less than): capture rate > 98%; accuracy of recognition of the direction of movement of the car > 96%; false capture rate <2% (entry/exit), <5% (checkpoint); European and Russian-speaking regions: LPR accuracy > 98%; country/region recognition accuracy > 98%. • vehicle type recognition (not exclusively, but including): car (including SUV, minibus, pickup truck)/truck/bus/minibus. • storage method (not less than): Micro SD card up to 128GB. • audio interfaces (not less than): 1 audio output. • alarm interfaces (not less than): 2 inputs. • network interfaces (not less than): 1 RJ45 10M / 100M / 1000M. • power supply (not less than): 12V DC. • PoE (not less than): PoE (802.3af). • power consumption (not worse): 20 W. • working temperature (not worse): -30 ° C - 70 ° C.

	• degree of protection (not less than): IP67, IK10.
The fisheye video camera must have technical and other characteristics per the following requirements (not less than):	• lens (not less than): 1 / 1.8" Progressive Scan CMOS. • maximum resolution (not worse): 3072x2048. • minimum sensitivity (not less than): Color: 0.047 Lux / F2.6 (AGC included), B/W: Color: 0.0047 Lux / F2.6 (AGC included), 0 Lux with IR. • shutter speed (not less than): 1s-1 / 100,000s. • slow shutter support. • day/night mode (not less than): Auto (ICR) / Schedule / Start on alarm. • illumination type: IR. • backlight control (not less than): each LED is controlled independently. • number of diodes (not worse): 3. • illumination range (not less than): 15 m. • type of lens: "fisheye". • focal length (not less than): 1.27 mm. • lens mount: M12. • aperture (not less than): F2.6. • viewing angles (not less than): H: 180 ° (wall mounting), 360 ° (ceiling), 360 ° (tabletop). • video compression (not less than): H.265 / H.264 / MJPEG. • number of streams (not worse): 2 streams. • support for resolutions (not less than): 3072x2048, 2048x2048, 1280x1280, 720x720, 720x480. • frame rate (not worse): (mainstream) 3072x2048, 2048x2048, 1280x1280 - 25 k / s; (additional stream) 720x720, 720x480 - 25 k / s. • video bitrate (not worse): 32 Kbit / s - 16 Mbit / s. • Noise suppression (DNR) 3D-DNR ; • WDR (not worse): 120 dB. • support (not less than): BLC; HLC; ROI with support for 4 fixed areas for the mainstream; Defog; SVC with H.264 and H.265 encoding support. • image settings (not exclusively, but including): saturation, brightness, contrast, and sharpness with the possibility of adjustment by client software or web browser. • basic processing functions (not exclusively, but including): mirroring, private masks, image overlay. • audio compression (not exclusively but including): G.711 / G.722.1 / G.726 / MP2L2 / PCM. • audio bitrate (not worse): 64Kbit / s (G.711) / 16Kbit / s (G.722.1) / 16Kbit / s (G.726) / 32-160Kbit / s (MP2L2). • Ethernet (not worse): RJ45 (10M / 100M / 1000M). • network protocols (not exclusively, but including): TCP / IP,

	ICMP, HTTP, HTTPS, FTP, DHCP, DNS, DDNS, RTP, RTSP, RTCP, PPPoE, NTP, UPnP, SMTP, SNMP, IGMP, 802.1 X, QoS, IPv6, UDP, Bonjour. • compatibility (not exclusively, but including): ONVIF (PROFILE S, PROFILE G), ISAPI. • number of simultaneous connections (not worse): 20. • storage method (not less than): NAS (NFS, SMB / CIFS), ANR, Micro SD. • browser support (not exclusively, but including): IE8 +, Chrome 31.0-44, Firefox 30.0-51, Safari 8.0+. • mobile platforms (not less than): iOS, Android. • security (not exclusively, but including): password protection, HTTPS encryption, IEEE 802.1x port-based network access control, IP address filter, basic and digest authentication for HTTP / HTTPS, WSSE and digest authentication for ONVIF. • users/levels (not worse): up to 32 users; 3 levels: administrator, operator, and user. • display in real-time (not worse): 18 display modes. • mounting type (not less than): desktop, wall, ceiling. • decoding modes (not less than): hardware, software. • software decoding, ceiling mount (not worse): "fisheye", 180 panoramic views, 360 panoramic views, 360 panoramic + PTZ, 360 panoramic + 3PTZ, 360 panoramic + 6PTZ, 360 panoramic + 8PTZ, 2PTZ, 4PTZ, fisheye + 3PTZ, fisheye + 8 PTZ, hemisphere, AR hemisphere, cylinder. • software decoding, wall mounting (not worse): "fisheye", panoramic view, panorama + 3PTZ, panorama + 8PTZ, 4PTZ, "fisheye" + 3PTZ, "fisheye" +8 PTZ. • software decoding, desktop mount (not worse): "fisheye", 180 panoramic images, 360 panoramic, 360 panoramic + PTZ, 360 panoramic + 3PTZ, 360 panoramic + 6PTZ, 360 panoramic + 8PTZ, 4PTZ, "fish" fisheye" + 3PTZ, "fisheye" + 8 PTZ, cylinder. • hardware decoding, ceiling mount (not worse): "fisheye", 180 panoramic images, panoramic view, 4PTZ, "fisheye" + 3PTZ, 4PTZ fusion. • hardware decoding, wall mounting (not worse): "fisheye", 180 panoramic images, panoramic view, 4PTZ, "fisheye" + 3PTZ, 4PTZ fusion. • hardware decoding, desktop mount (not worse): "fisheye", 180 panoramic images, panoramic view, 4PTZ, "fisheye" + 3PTZ, 4PTZ fusion. • audio interfaces (not less than): 1 in / 1 out, 2 built-in microphones, 1 speaker, mono sound. • alarm interfaces (not less than): 1 in / 1 out. • network interfaces (not less than): 1xRJ45 10M / 100M / 1000M. • local memory (not less than): micro-SD / SDHC / SDXC up to

	256 GB. • the presence of a reset button. • alarm triggers (not exclusively, but including): motion detection, scene change, network disconnection, IP address conflict, illegal access, storage error. • SMART functions (not exclusively, but including): Line crossing; Invasion of the region; Entry and exit from the region; Abandoned / missing items; Detection of audio exceptions; Counting objects Counting people entering, leaving, and passing by; the ability to send reports by e-mail daily, weekly, monthly or annually. • support for target filtering by height. • heat map (not less than): graphic description of visits (calculated by the number of people or by time-out) in a given area. • power supply (not less than): DC 12V ± 20%, two-wire terminal block. • PoE (not worse): PoE (802.3at) (Class 4). • power consumption (not worse): DC 12V: 1 A, 12.5 W; PoE: (802.3at, 42.5-57 V), 0.4A - 0.3A, max. 15 W. • working temperature (not worse): -40 ° C - + 60 ° C. • humidity (not less than): <95%. • degree of protection (not less than): IP67, IK8. • material (not less than): metal. • availability of heating.
Video camera with type 2 license plate recognition must have technical and other characteristics per the following requirements (not less than):	• a matrix not less than 2 MP (1/1.8 '' CMOS). • maximum resolution, not worse: 1920×1080. • focal length, not less than 8~32 mm. • shutter speed, not less than 1-1/100,000s, with slow shutter support. • day/night mode: IR filter. • IR range, not worse: up to 80 m. • minimum light sensitivity, not worse: Color: 0.001 lux @ (F1.2, AGC ON); B/W: 0.0001 Lux with IR. • video compression standards, not less than mainstream video compression: H.265 / H.264 / MJPEG; sub stream: H.265 / H.264 / MJPEG; H.264: basic profile / main profile / high profile; H.265: basic profile / main profile / high profile. • video transmission speed, not worse: mainstream 1080p, 50 frames per second. • number of streams, not worse: mainstream (not worse): 50 Hz: 50 frames per second (1920 × 1080, 1280 × 720, 704 × 576, 352 × 288); 60 Hz: 30 frames per second (1920 × 1080, 1280 × 720, 704 × 576, 352 × 288); additional stream: 50 Hz: 25 frames per second (1920 × 1080, 1280 × 720, 704 × 576, 352 × 288); 60 Hz: 30 frames per second (1920 × 1080, 1280 × 720, 704 × 576, 352

	× 288); third stream 50 Hz: 25 frames per second (1280 × 720, 704 × 576, 352 × 288); 60 Hz: 30 frames per second (1280 × 720, 704 × 480, 640 × 480); • automatic switch (not less than): day/night / scheduled / triggering of the alarm signal. • storage, not less than MicroSD / TF-card network storage (128 GB). • automatic download of the archive if the network disappears (ANR), not less than supports. • simultaneous live viewing, not worse: up to 20 channels. • the presence of a reset button. • support for image enhancement, not worse: BLC, HLC, 3D DNR, Defog, EIS. • area of operation, not less than 2 traffic lanes. • basic functions, not less than vehicle license plate recognition; recognition of vehicles without license plates; support for motorcycle license plate recognition; support for detecting vehicle attributes, including vehicle type, color, brand, etc. • operating conditions, not worse: from -40°C to 60°C. • power, current, and PoE support, not less than 12 V DC, max. 18.0W PoE: (802.3at). • protection against dust and water, not worse: IK10, IP67.
The video camera is robotic and must have technical and other characteristics per the following requirements (not less than):	• Matrix : 1/2.5 '' Progressive Scan CMOS • Color sensitivity: 0.005 lux (AGC included), B/W: 0.001 lux (AGC included), 0 lux with IR. • Electronic shutter speed: 1s ~ 30000s. • Day/night mode: mechanical IR filter. • Lens: focal length 4.8-153 mm, optical zoom 32x, digital zoom 16x, zoom speed 5.6 s. • Focusing: auto/semi-automatic/manual. • Auto tracking: manual activation, automatic tracking of an object (setting of special targets - a person or a vehicle, upon activation of Smart-detections). • Patrols: 8 zones, up to 32 presets in each. • Support for PTZ position display. • Idle actions: preset, patrol, template, auto scan, vertical scan, pan scan, random scan, frame scan. • Scheduled actions: preset, patrol, pattern call, auto scan, vertical scan, pan scan, frame scan, reboot, initialize. • Smart video analytics: detection of unauthorized actions, network disruption, IP address conflict, and storage errors. • Alarm actions: pre-setting, patrolling, pattern calling, recording to microSD / SDHC card, relay activation, client message, sending e-mail, uploading to FTP, activating the recording channel.

	• Compression: video compression mainstream: H.265 / H.264, secondary stream: H.265 / H.264 / MJPEG, third stream: H.265 / H.264 / MJPEG. • Audio compression: G.711ulaw / G.711alaw / G.726 / MP2L2 / G.722. • Maximum image resolution (not less than): 1920×1080. • SVC support. • Image enhancement: hardware WDR 120dB, 3D DNR, BLC, HLC, anti-fog, ROI. • Day/night switching: auto/scheduled/alarmed. • Smart video analytics: motion detection, detection of line crossing, intrusion into the area, entry/exit from the area, abandoned / missing objects, support for triggering alarms by different types of objects (person or vehicle), support for filtering false alarms caused by leaves, light, animals, etc., anti-sabotage, detection of a change in the storied program, exceeding/underestimating the sound threshold, audio loss, defocusing, object recognition, person detection; • Network storage: NAS, ANR. • Protocols: IPv4 / IPv6, HTTP, HTTPS, 802.1x, Qos, FTP, SMTP, UPnP, SNMP, DNS, DDNS, NTP, RTSP, RTCP, RTP, TCP / IP, DHCP, PPPoE, Bonjour. • frame rate (including but not limited to): mainstream: 2560x1440 - 25 fps, 1920x1080 - 50 fps. • Local memory: a slot for microSD / SDHC up to 256GB. • Power supply: AC24V; HI-PoE Max. 30W • Operating temperature regime: -30°C ~ +65°C. • Humidity: 90% or less. • Protection: IP67, IK10, TVS 4000V.
Monitoring video camera must have technical and other characteristics per the following requirements (not less than):	• lens (not less than): 1 / 2.7 "Progressive Scan CMOS. • maximum resolution: not less than 2592 × 1944. • minimum sensitivity: not less than than 0.003 lux @ (F1.4, AGC ON). • shutter speed: not worse than from 1/3 s to 1/100000 s. • support for slow shutter speed. • WDR: not less than than 120 dB. • day/night mode: not less than an IR filter. • adjustment of angles (not less than): pan: from 0 ° to 360 °, tilt: from 0 ° to 90 °, rotation: from 0 ° to 360 °. • lens mount: M12. • lens type (not less than): 2.8 mm. • aperture not worse: F1.4. • IR range (not less than): up to 40 m. • wavelength (not worse): 850 nm. • availability of intelligent additional lighting.

	• frame rate (including but not limited to): main stream: 50 Hz: 20 frames per second (2592 × 1944); 25 frames per second (2688 × 1520, 2304 × 1296, 1920 × 1080, 1280 × 720); 60 Hz: 20 frames per second (2592 × 1944); 30 frames per second (2688 × 1520, 2304 × 1296, 1920 × 1080, 1280 × 720); additional stream: 50 Hz: 25 fps (640 × 480, 640 × 360, 320 × 240); 60 Hz: 30 frames per second (640 × 480, 640 × 360, 320 × 240); third stream 50 Hz: 15 frames per second (1280 × 720, 640 × 480, 640 × 360, 320 × 240); 60 Hz: 15 frames per second (1280 × 720, 640 × 480, 640 × 360, 320 × 240); fourth stream: 50 Hz: 15 fps (1280 × 720, 640 × 480, 640 × 360, 320 × 240); 60 Hz: 15 frames per second (1280 × 720, 640 × 480, 640 × 360, 320 × 240) (supported in certain settings); • video compression (not worse): mainstream: H.265 / H.264 additional stream: H.265 / H.264 / MJPEG; third stream: H.265 / H.264; fourth stream: H.265 / H.264 / MJPEG (support under certain settings). • video bitrate (not worse): 32 Kbit / s to 8 Mbit / s. • H.264 type (not less than): Basic profile / Basic profile / High profile. • H.265 type (not worse): Basic profile. • data transfer speed control (not less than): CBR / VBR. • SVC support. • ROI (not less than): 5 fixed regions for the mainstream and additional stream. • presence of environmental noise filtering function. • audio sampling frequency (including, but not limited to): 8 kHz / 16 kHz / 32 kHz / 44.1 kHz / 48 kHz. • sound compression (including, but not limited to): G.711ulaw / G.711alaw / G.722.1 / G.726 / MP2L2 / PCM / MP3. • audio transmission rate (including, but not limited to): 64 Kbps (G.711ulaw / G.711alaw) / 16 Kbps (G.722.1) / 16 Kbps (G.726) / 32- 192 Kbps (MP2L2) /8-320 Kbps (MP3). • possibility of simultaneous live viewing of at least 6 channels. • API (including, but not limited to): ONVI F (PROFILE S, PROFILE G), ISAPI, SDK. • protocols (including but not limited to): TCP / IP, ICMP, HTTP, HTTPS, FTP, DHCP, DNS, DDNS, RTP, RTSP, NTP, UPnP, SMTP, IGMP, 802.1X, QoS, IPv6, UDP, Bonjour, SSL / TLS, PPPoE. • user/host (not worse): up to 32 users; 3 user levels: administrator, operator, and user. • security (including but not limited to): password protection, complex password, HTTPS encryption, IP address filter, security audit log, basic and digest authentication for HTTP / HTTPS, TLS 1.2, WSSE, and digest authentication for interface Open Network

	Video. • network storage (not less than): MicroSD / SDHC / SDXC card (256 GB), local memory and NAS (NFS, SMB / CIFS), ANR. • support for web browsers (including, but not limited to): IE 10, IE 11, Chrome 57.0+, Firefox 52.0+, and Firefox 52.0+. • switching day/night (not less than): day, night, auto, schedule. • availability of target crop function. • image enhancement (including, but not limited to): BLC, HLC, 3D DNR. • the presence of a switch for image parameters. • image settings (including, but not limited to): rotation mode, saturation, brightness, contrast, sharpness, gain, and white balance adjusted by client software or web browser. • signaling (not less than): 1 input, 1 output (max. 12 V DC, 30 mA). • audio (not worse): 1 input (line input), max. input amplitude: 3.3 vpp, input impedance: 4.7 kΩ, interface type: unbalanced; 1 output (line output), max. output amplitude: 2.5 vpp, output impedance: 100 ohms, interface type: unbalanced, mono sound. • built-in storage (not less than): built-in micro-SD / SDHC / SDXC slot, up to 256 GB. • the presence of a reset button. • output power (not worse): 12 V DC, max. 100 mA (with support for all types of power sources). • support for Smart functions (including but not limited to): main event: motion detection, video tampering alarm, exception (network disconnected, IP address conflict, illegal login, hard disk full, hard disk error), scene change detection; intelligent (deep learning algorithm): face capture; line crossing detection, intrusion detection, region entry detection, region exit detection; • storage method (including, but not limited to): NAS / memory card, message to the monitoring center, start recording, capture. • availability of functions (including, but not limited to): anti-flicker, heartbeat, mirror, privacy masks, flash log, password reset by e-mail, and pixel counter. • availability of software reset function. • operating temperature in the range not worse than: from -30 ° C to 60 ° C. • humidity 95% or less (without condensation). • power supply unit (not less than): 12 V DC ± 25%; PoE: 802.3af, Type 1, Class 3. • consumed power and current (not less than): max. 7.2 W, 12 V, 0.6 A; PoE (802.3af, 36 V to 57 V), 0.3 A to 0.2 A, max. 8.5 W. • degree of protection not less than IP67 (IEC 60529-2013).
The bracket for a video camera with	• type: rack bracket for video cameras with license plate recognition for entrances/exits.

license plate recognition type 1 must have technical and other characteristics per the following requirements (not less than):	• availability of floor attachment. • height from the floor (not less than): 1450 mm. • material (not less than): aluminum alloy. • compatibility with a video camera, the requirements for which are set out in clause 2.2.6.1.
Fish-Eye Camcorder Bracket must have technical and other characteristics per the following requirements (not less than):	• type: wall mounting bracket for fisheye video cameras. • adjustment angle (not less than): panning: 360 °; slope: 100 °; rotation: 360 °. • size (no more): 164x153x199 mm. • material (not less than): aluminum alloy. • compatibility with the video camera, the requirements for which are set out in clause 2.2.6.2.
The switching box must have technical and other characteristics per the following requirements (not less than):	• material (not less than): aluminum alloy. • maximum load capacity of the bracket (not worse): 4.5 kg. • dimensions: Ø 137x53x164 mm.
Memory cards must have technical and other characteristics per the following requirements (not less than):	• card class (not less than): Class 10. • memory capacity (not worse): 32 GB. • recording speed (not worse): 25 Mb / s. • reading speed (not worse): 90MB/s. • memory standard: micro-SD.
Box for installing network equipment the set must have technical and other characteristics per the following	• 2 cables inputs. • degree of protection: IP54. • execution type: wall-mounted, with clamps for fastening to a pole. • maximum static load: not less than 5 kg. • mounting rack made of sheet steel. • sliding lock. • sockets 220V type C1-a according to GOST 7396.1-89.

requirements (not less than):	• dimensions (no more): 500x400x250 (HxWxD), mm.
Column brackets must have technical and other characteristics per the following requirements (not less than):	• purpose: for mounting on a pole. • support for mounting on a pole diameter from 70 to 120 mm. • body material (not less than): galvanized steel.
The switch is controlled by 24 optical ports and must have technical and other characteristics per the following requirements (not less than):	• Ethernet ports (Uplink) (not worse): 24x SFP (1000M). • Ethernet ports (Downlink) (not worse): 24x SFP (10G). • additional OOB ports (no less than): 1x RJ45 (control only); Console: 1x RJ45-R232 (115200.8, N, 1). • transmission distance (no less than): RJ45 - 100 meters, SFP depending on the type of module. • availability of voltage monitoring. • VLAN support. • port mirroring support. • management (no less than): Web / CLI Management L2 / L3. • presence of a COM port. • maximum bandwidth (no less than): 128Gbps. • packet forwarding speed (not worse): 95.2Mpps. • buffer memory (no less than): 12Mb. • MAC table size (no less than): 16K. • power supply (no less than): AC 100V ~ 240V. • power consumption (no less than): 60W. • working temperature (not worse): 10 ℃ ~ 50 ℃. • humidity (no less than): 0 ~ 95%. • Level 2 feature set support: • VLAN, IEEE 802.1Q Trunking, vPC (or similar), Link Aggregation Control Protocol (LACP), Unidirectional Link Detection (UDLD; standard and aggressive), Multiple Spanning Tree Protocol (MSTP), Rapid Spanning Tree Protocol (RSTP), Spanning Tree Protocol guards, and Transparent VLAN Trunk Protocol (VTP). • Security: Authentication, Authorization, and Accounting (AAA); Dynamic Host Configuration Protocol (DHCP) snooping; storm control; configurable Control-Plane Policing (CoPP); and private VLAN (PVLAN). • Support for Nexus Dashboard Fabric Controller 12 or equivalent, Secure Shell Version 2 (SSHv2) access, Cisco Discovery Protocol, SNMP and SYSLOG. • Support for IPv4 Routing (level 3): • Static Routes.

	• HSRP (v1, v2) or VRRP. • RIP. • BGP, EIGRP, GRE, IS-IS, MSDP, OSPF, PBR, PIM, SSM, VRF3, VXLAN BGP EVPN, Micro-segmentation (using VXLAN Group Policy Option), SRv6 (no EVPN), and SR-MPLS (no EVPN). • And also support for such functionality (not worse) — iCAM, ITD, IP fabric for media non-blocking multicast, and smart channel), NetFlow, FT, FTE, SSX), DCI overlay features (Inter-AS option B, segment routing SR- MPLS, Layer 3 EVPN over segment routing SRv6, MPLS Layer 3 VPN, and VXLAN EVPN Multi-Site), (Enhanced PBR (EPBR)), RTP Flow Monitoring (Media Flow Analytics), PTP Monitoring, Multicast NAT. • Mandatory support for SDN technology, which must include a software solution that in turn must provide the customer with a holistic, purpose-driven architecture with centralized automation and policy-based application profiles, such as Cisco's Application Centric Infrastructure (ACI) solution. (or equivalent). • The SDN solution must be from the same manufacturer as the equipment manufacturer in the proposal. • A Cisco ACI solution (or equivalent) should be built on a two-tier architecture based on the Clos Network principle and should provide a reliable transport network for dynamic workloads while eliminating points of failure, anti-loop protocols (STP), traffic bottlenecks, and problems with scalability, as well as increase the overall bandwidth of the entire network. • The ACI software architecture (or equivalent) should allow the creation of granular control objects (network, "VLAN", group of end devices based on some criterion) between which interactions can be controlled. The ACI software (or equivalent) should allow creating service chains, with the redirection of a certain (or all) type of traffic to a virtual or physical security device, for additional traffic control and between server and service interaction. • Also, the Cisco ACI solution (or equivalent) should provide the ability to integrate both with Cisco Firepower security devices and with various virtual infrastructures, including VMware, Hyper-V, KVM, and container environments. • Integration with Cisco Firepower security appliances enables mutual addition of objects (describing users or end resources, in access policies) from Cisco ACI (or equivalent) to Cisco Firepower Management Center (FMC) and vice versa, which in turn reduces the likelihood of errors in setting up or maintaining the data center system. • The goal of integration with different virtual infrastructures is to be able to apply a single ACI policy model (or equivalent) to both physical and virtual environments and to be able to implement

	access policies between different end devices from a single point, the ACI management window, regardless of whether they are located locally at the customer or remotely, whether they are physical or virtual.
The PoE switch is controlled by 16 ports and must have technical and other characteristics per the following requirements (not less than):	• Copper ports (no less than): 16*10/100/1000Base-T PoE RJ45 (Auto-MDI/MDI-X). • SFP ports (no less than): 4*1000M/10G Base-X SFP (Mini-GBIC). • console port (no less than): 1*serial port RJ45-R232 (115200.8, N, 1). • PoE standard (no less than): IEEE 802.3af/at (PSE). • PoE output power (not worse): 46 ~ 55 V DC. • PoE power supply (no less than): max. 30 W per port, max. 360 W. • recommended support for data stacking technologies through separate or network ports. • standards (not exclusively, but including): IEEE 802.3, IEEE 802.3u, IEEE 802.3ab, IEEE 802.3z, IEEE 802.3x, IEEE 802.1Q, IEEE 802.1p, IEEE 802.3ad, IEEE 802.1D, IEEE 802.1x. • forwarding modes (no less than): storage and forwarding. • packet buffer (not worse): 12 Mbit. • MAC table (not worse): 16K, with support for automatic learning. • switching capacity (not worse): 112 Gbit / s. • packet forwarding speed (not worse): 83.3pps. • input voltage (not worse): power supply 1 (main): 48 ~ 57 V DC, power supply 2 (backup): 48 ~ 57 V DC. • energy consumption (not worse): 380 W (including PoE). • reliability (no less than): 6 kV, standard: IEC6000-4-5; protection against electrostatic discharge: contact discharge 8 kV, air discharge 15 kV, standard: IEC61000-4-2. • protection level (no less than): IP40. • working temperature (not worse): -40 ~ 75 ℃. • support for two DC power supplies. • support for connecting expansion modules with Ethernet ports. • working humidity (not worse): 0 ~ 95% (without condensation). • LED indicators (no less than): indicator of the main power source; reserve power supply indicator; system operation indicator; alarm indicator. • material (no less than): aluminum. • installation (no less than): DIN rail or wall. • Support for such functionality (no less than) — IEEE 802.1, 802.3 standard, NTP, UDLD, CDP, LLDP, unicast MAC filter, PAgP, LACP VTPv2, VTPv3, EtherChannel, Q-in-Q tunneling, voice VLAN, PVST+, MSTP, and RSTP, IGMPv1, v2, v3 snooping, IGMP filtering, IGMP querier, WebUI, MIB, SmartPort, SNMP, syslog, DHCP server, SPAN session, RSPAN, FSPAN, Express

	setup, NETCONF, RESTCONF, Port security, 802.1x, Dynamic Host Configuration Protocol (DHCP) snooping, dynamic ARP inspection, IP source guard, guest VLAN, MAC authentication bypass, 802.1x multidomain authentication, storm control - unicast, multicast, broadcast, SCP, SSH, SNMPv3, TACACS+, RADIUS server/client, MAC address notification, BPDU guard, Access Lists (PACL,VACL,RACL), SUDI 2099 (Secure Unique Device identifier), Full Flexible NetFlow (FNF), MACsec-128, FIPS 140-2, Ingress policing, rate limit, egress queuing and shaping, auto QoS, IPv6 host support, SNMP over IPv6, HTTP/HTTP(s) over IPv6, SNMP over IPv6, Syslog over IPv6, DHCPv6 relay source, DHCPv6 bulk lease query (RFC 5460), IPv6 stateless Auto Config SCP/ SSH, Radius, TACACS+, NTP over IPv6, IPv6 VRF aware BGPv6, IPV6 ND cache expire, IPv6 support for TFTP, IPv6 DNS transport, IPv6 QoS, IPv6 FHS RA Guard, IPv6 FHS DHCPv6 Guard, Inter-VLAN routing, Static routing, CIP Ethernet/IP, IEEE 1588 PTP v2 (default and power), PROFINET, Resilient Ethernet Protocol (REP) ring, PROFINET-Media Redundancy Protocol (MRP), REP Preferred, Fast REP, Dying gasp, SCADA protocol classification - GOOSE messaging, MODBUS TCP/IP, YANG, NETCONF, RESTCONF, Layer 2 switching with 1:1 switch Network Address Translation (L2NAT). • Support for SDN technology for corporate or industrial networks, namely the Cisco SD-Access architecture (or equivalent). • The equipment must support at least 1 Virtual Network (VN) and the ability to perform such roles in the SD-Access factory as Fabric Border and Control Plane and Fabric Extended. • The factory Cisco SD-Access controller (or equivalent) must be free and available to download in virtual form for private on-premises deployment in a VMware vSphere (ESXi) virtualization system.
The PoE switch is controlled by 8 ports and must have technical and other characteristics per the following requirements (not less than):	• Copper ports (not worse): 8*10/100/1000Base-T PoE RJ45 (Auto-MDI/MDI-X). • SFP ports (no less than): 4*1000M/10G Base-X SFP(Mini-GBIC). • console port (no less than): 1*serial port RJ45-R232 (115200.8, N, 1). • PoE standard (no less than): IEEE 802.3af/at (PSE). • PoE output power (not worse): 46 ~ 55 V DC. • PoE power supply (no less than): max. 30 W per port, max. 240 W. • standards (not exclusively, but including): IEEE 802.3, IEEE 802.3u, IEEE 802.3ab, IEEE 802.3z, IEEE 802.3x, IEEE 802.1Q, IEEE 802.1p, IEEE 802.3ad, IEEE 802.1D, IEEE 802.1x. • recommended support for data stacking technologies through separate or network ports. • forwarding modes (no less than): storage and forwarding.

	• packet buffer (not worse): 12 Mbit. • MAC table (not worse): 16K, with support for automatic learning. • switching capacity (not worse): 96 Gbit / s. • packet forwarding speed (not worse): 71.4pps. • input voltage (not worse): power supply 1 (main): 48 ~ 57 V DC, power supply 2 (backup): 48 ~ 57 V DC. • energy consumption (no less than): 260 W (including PoE). • reliability (no less than): 6 kV, standard: IEC6000-4-5; protection against electrostatic discharge: contact discharge 8 kV, air discharge 15 kV, standard: IEC61000-4-2. • protection level (no less than): IP40. • working temperature (not worse): -40 ~ 75 ℃. • support for two DC power supplies. • support for connecting expansion modules with Ethernet ports. • working humidity (not worse): 0 ~ 95% (without condensation). • LED indicators (no less than): indicator of the main power source; reserve power supply indicator; system operation indicator; alarm indicator. • material (no less than): aluminum. • installation (no less than): DIN rail or wall. • Support for such functionality (no less than) — IEEE 802.1, 802.3 standard, NTP, UDLD, CDP, LLDP, unicast MAC filter, PAgP, LACP VTPv2, VTPv3, EtherChannel, Q-in-Q tunneling, voice VLAN, PVST+, MSTP, and RSTP, IGMPv1, v2, v3 snooping, IGMP filtering, IGMP querier, WebUI, MIB, SmartPort, SNMP, syslog, DHCP server, SPAN session, RSPAN, FSPAN, Express setup, NETCONF, RESTCONF, Port security, 802.1x, Dynamic Host Configuration Protocol (DHCP) snooping, dynamic ARP inspection, IP source guard, guest VLAN, MAC authentication bypass, 802.1x multidomain authentication, storm control - unicast, multicast, broadcast, SCP, SSH, SNMPv3, TACACS+, RADIUS server/client, MAC address notification, BPDU guard, Access Lists (PACL,VACL,RACL), SUDI 2099 (Secure Unique Device identifier), Full Flexible NetFlow (FNF), MACsec-128, FIPS 140-2, Ingress policing, rate limit, egress queuing and shaping, auto QoS, IPv6 host support, SNMP over IPv6, HTTP/HTTP(s) over IPv6, SNMP over IPv6, Syslog over IPv6, DHCPv6 relay source, DHCPv6 bulk lease query (RFC 5460), IPv6 stateless Auto Config SCP/ SSH, Radius, TACACS+, NTP over IPv6, IPv6 VRF aware BGPv6, IPV6 ND cache expire, IPv6 support for TFTP, IPv6 DNS transport, IPv6 QoS, IPv6 FHS RA Guard, IPv6 FHS DHCPv6 Guard, Inter-VLAN routing, Static routing, CIP Ethernet/IP, IEEE 1588 PTP v2 (default and power), PROFINET, Resilient Ethernet Protocol (REP) ring, PROFINET-Media Redundancy Protocol (MRP), REP Preferred, Fast REP, Dying gasp, SCADA protocol classification - GOOSE messaging,

	MODBUS TCP/IP, YANG, NETCONF, RESTCONF, Layer 2 switching with 1:1 switch Network Address Translation (L2NAT). • Support for SDN technology for corporate or industrial networks, namely the Cisco SD-Access architecture (or equivalent). • The equipment must support at least 1 Virtual Network (VN) and the ability to perform such roles in the SD-Access factory as Fabric Border and Control Plane and Fabric Extended. • The factory Cisco SD-Access controller (or equivalent) must be free and available to download in virtual form for private on-premises deployment in a VMware vSphere (ESXi) virtualization system.
A set of SFP modules must have technical and other characteristics per the following requirements (not less than):	• data transfer speed (not worse): 1 Gbit / s. • distance (no less than): up to 20 km. • connector type: LC UPC. • format: SFP. • be compatible with the equipment specified in these technical requirements and the existing equipment from this manufacturer. • the compatibility of the equipment must be confirmed on the website of the equipment manufacturer.
FP to 1000BASE-T converter must have technical and other characteristics per the following requirements (not less than):	• device type: SFP optical module. • Ethernet port (not worse): 1 x 1000 Mbit / s. • SFP port (not worse): 1 x 1000 Mbit / s. • bandwidth (not worse): 1000 Mbit / s. • standard: IEEE 802.3. • Ethernet port (not worse): RJ-45 (10/100/1000 BASE-T); compatible with MSA SFP. • maximum signal transmission distance (not less than): up to 100 meters. • compliance with the IEEE Std 802.3 standard. • hot swapping support. • power supply (not less than): DC 3.15-3.45V. • consumption (not less than): 1 W. • electrostatic protection (ESD) of the IEC61000-4-2 standard. • temperature range (not less than): 0 ° C ~ + 70 ° C. • humidity (not less than): up to 95%.
Access card reader with keyboard must have technical and other characteristics per the following requirements (not	• method of operation: RFID reader. • processor (not less than): 32-bit. • power supply (not less than): 12V DC. • power consumption (not less than): ≤500mA. • connection interface (not less than): RS485 or Wiegand (W26 / W34). • card type: Mifare. • frequency characteristic: 13.56MHz.

less than):	• reading distance (not less than): ≤50mm. • ID setting (not less than): through DIP switches. • presence of audio indication. • keyboard (not less than): with 12 keys (from 0 to 9, *, #). • availability of state indication. • availability of anti-sabotage tamper. • working temperature (not worse): -20 ° C to + 65 ° C. • humidity (not less than): 10% to 90%. • degree of protection (not less than): IP65. • installation (not less than): overhead.
Mifare contactless card with chip must have technical and other characteristics per the following requirements (not less than):	• type of device: card with a chip. • frequency response: 13.56 MHz • material: PVC. • dimensions (no more): 85x54x0.84 mm.
Controller for 2 barriers must have technical and other characteristics per the following requirements (not less than):	• processor (not less than): 32-bit high-speed processor. • number of barriers (not worse): 2. • communication interface: TCP / IP. • connection interface (not less than): RS-485, Wiegand. • card memory (not less than): 100,000; Events: 300,000. • status indication (not less than): power supply status, communication status, working status. • wall reader (not less than): via Wiegand (4 readers) or RS485 (up to 8 readers). • output interfaces (not worse): blocking relay x4, alarm relay x4. • power consumption (not less than): ≤100 W. • working temperature (not less than): -20 ° C - +65 ° C.
The battery must have technical and other characteristics per the following requirements (not less than):	• type: AGM technology. • capacity (not less than) 7Ah. • voltage (not less than) 12V.
The barrier must have technical and other characteristics per	• boom length (at least): 3 meters. • opening time (no more): 5 s. • input interface: 8 digital. • power consumption (not less than): ≤100 W.

the following requirements (not less than):	• working temperature (not worse): -20 ° C - +55 ° C.
Type 1 traffic light must have technical and other characteristics per the following requirements (not less than):	• the parameters of the traffic light must comply with the norms of DSTU 4092-2002. • the maximum duration of measured signals (not less than): 255 seconds. • interval measurement error: no more than 1 sec. • supply voltage (not worse): 220V (+22 / -33) 50Hz. • average power consumed by one section: no more than 7 W. • the traffic light must ensure the stability of light technical parameters during the entire period of operation in the range of supply voltages from 187V to 242V. • body (not less than): made of black polycarbonate. • frontal lenses of the modules (not less than): colorless and eliminate phantom illumination. • degree of protection (not less than): IP65. • temperature during operation (not less than): from -40 ° C to + 70 ° C. • the design of the traffic light should provide for the attachment of additional sections to it. • the design of the traffic light should allow it to be attached to all types of consoles, walls, and stretchers. • service life: at least 10 years.
Type 2 traffic lights must have technical and other characteristics per the following requirements (not less than):	• type: reversionary. • the parameters of the traffic light must comply with the norms of DSTU 4092-2002. • the maximum duration of measured signals (not less than): 255 seconds. • interval measurement error: no more than 1 sec. • supply voltage (not worse): 220V (+22 / -33) 50Hz. • average power consumed by one section: no more than 7 W. • the traffic light must ensure the stability of light technical parameters during the entire period of operation in the range of supply voltages from 187V to 242V. • body (not less than): made of black polycarbonate. • frontal lenses of the modules (not less than): colorless and eliminate phantom illumination. • degree of protection (not less than): IP65. • temperature during operation (not less than): from -40 ° C to + 70 ° C. • the design of the traffic light should provide for the attachment of additional sections to it. • the design of the traffic light should allow it to be attached to all

	types of consoles, walls, and stretchers. • service life: at least 10 years.
Traffic video camera for monitoring the queue when leaving the PP in Poland must have technical and other characteristics per the following requirements (not less than):	• a matrix not less than 2 MP (1/1.8 '' CMOS). • maximum resolution, not worse: 1920×1080. • focal length, not less than 8~32 mm. • shutter speed, not less than 1-1/100,000s, with slow shutter support. • day/night mode: IR filter. • IR range, not worse: up to 50 m. • minimum light sensitivity, not worse: Color: 0.001 lux @ (F1.2, AGC ON); B/W: 0.0005 Lux with IR. • video compression standards, not less than mainstream video compression: H.265 / H.264 / MJPEG; sub stream: H.265 / H.264 / MJPEG; H.264: basic profile / main profile / high profile; H.265: basic profile / main profile / high profile. • video transmission speed, not worse: mainstream 1080p, 50 frames per second. • number of streams, not worse: mainstream (not worse): 50 Hz: 50 frames per second (1920 × 1080, 1280 × 720, 704 × 576, 352 × 288); 60 Hz: 30 frames per second (1920 × 1080, 1280 × 720, 704 × 576, 352 × 288); additional stream: 50 Hz: 25 frames per second (1920 × 1080, 1280 × 720, 704 × 576, 352 × 288); 60 Hz: 30 frames per second (1920 × 1080, 1280 × 720, 704 × 576, 352 × 288); third stream 50 Hz: 25 frames per second (1280 × 720, 704 × 576, 352 × 288); 60 Hz: 30 frames per second (1280 × 720, 704 × 480, 640 × 480); • automatic switch (not less than): day/night / scheduled / triggering of the alarm signal. • storage, not less than MicroSD / TF-card network storage (128 GB). • automatic download of the archive if the network disappears (ANR), not less than supports. • simultaneous live viewing, not worse: up to 20 channels. • the presence of a reset button. • support for image enhancement, not worse: BLC, HLC, 3D DNR, Defog, EIS. • operating conditions, not worse: from -30°C to 70°C. • power, current, and PoE support, not less than 12 V DC, max. 15.0W PoE: (802.3at). • protection against dust and water, not worse: IK10, IP67.
The information panel must have technical and other	• brightness: 5000 nits. • pixel configuration: 3 in 1 SMD. • visual viewing angle (horizontal): 160°. • visual viewing angle (vertical): 130°.

characteristics per the following requirements (not less than):	• color temperature: from 3500 to 9000 K. • unit resolution (HxW pixels): 96x96 • power consumption per m²: up to 650 W. • power supply: 100-240 V AC • LED service life (half brightness): 100,000 hours • body material: aluminum. • unit area: 1 m² • operating conditions, not worse: from -20°C to 50°C. • protection class: IP65
Electric cable type 1 must have technical and other characteristics per the following requirements (not less than):	• number of veins: 3. • section: 1.5 sq. mm. • core material: copper. • shell: PVC. • insulation: PVC. • operating temperature: from -50 ° C to +50 ° C. • resistance to burning does not spread burning during single and bundle laying.
Type 2 electric cable must have technical and other characteristics per the following requirements (not less than):	• number of veins: 3. • section: 2.5 sq. mm. • core material: copper. • shell: PVC. • insulation: PVC. • operating temperature: from -50 ° C to +50 ° C. • resistance to burning does not spread burning during single and bundle laying.
Electric cable type 3 must have technical and other characteristics per the following requirements (not less than):	• number of veins: 3. • section: 4 sq. mm. • core material: copper. • shell: PVC. • insulation: PVC. • operating temperature: from -50 ° C to +50 ° C. • resistance to burning does not spread burning during single and bundle laying.
The pipe is two-layer and must have technical and other characteristics per the following requirements (not less than):	• outer diameter: 40 mm. • internal diameter: 32 mm. • operating temperature (not worse): from -45 ° C to + 60 ° C. • material (not less than): external case - HDPE; inner case - PVD. • type: flexible two-layer pipe.

Outdoor twisted pair cable must have technical and other characteristics per the following requirements (not less than):	• number of pairs: 4. • conductor material (not less than): copper. • cross-section (not less than): 0.50 mm. • installation type: street.
Type 1 fiber optic cable must have technical and other characteristics per the following requirements (not less than):	• number of fibers: 8. • cable diameter: 5.4 ± 0.2 mm. • diameter of the tube (tube): 2.3 ± 0.2 mm. • attenuation coefficient at reference wavelengths (not less than): - 1310nm / -1550nm 0.4 / 0.3 dB / km. • coefficient of chromatic dispersion at reference wavelengths (not less than): 18.6 / 23.7 ps / (nm, km). • permissible tensile force (not less than): 1 kN.
Type 2 fiber optic cable must have technical and other characteristics per the following requirements (not less than):	• number of fibers: 2. • outer shell: polyethylene. • permissible tensile force (not worse): 1.2 kN. • cable diameter (not less than): 5.4 mm. • central power element: fiberglass threads. • peripheral power element: fiberglass rods. • type: monotube. • fiber type: single-mode. • working temperature (not worse): from - 20 ℃ to + 60 ℃. • minimum bending radius (not worse): 20 mm. • attenuation coefficient of waves 1310 nm / 1550 nm (not worse): 0.36 / 0.22 dB / km.
"P" similar truss structure must have technical and other characteristics per the following requirements (not less than):	• Material – metal. • Width – 8 - 60 m. • Height - 4.5 - 6 m.
Installation set - the type and dimensions of the installation set are specified at the	• set of connectors: 1 set. • a set of consumables (screws, bolts, self-tapping screws, dowels, drills, etc.).

stage of the inspection of the air conditioning system installation objects, and it is preliminarily composed of the following parts:	

Detailed specifications: Monitoring Center Equipment and Software Requirements (Kyiv)

General requirements

- for the system of situational control of checkpoints for road traffic of the State Customs Service.
- the possibility of integration of SITMS built on various software, the most widespread on the market of Ukraine (not exclusively, but necessarily Milestone, Avigilon) with the help of ARI.
- the possibility of integration with the databases of the State Customs Service and other state bodies based on the available SDK.
- possibility of analysis, organization of response, investigation, reconstruction of the incident, and analysis of information.
- implementation of standard operating procedures based on specific policies and rules.
- optimization of standard operations.
- increased operational efficiency, which can be measured in the processing of more incidents and investigations per operator, as well as incidents that can be prevented.
- scalability of the solution when deploying new SITMS.
- the possibility of implementing incident response scenarios.
- collection, accumulation, and display of statistical data by various indicators and time intervals.
- automatic or manual dispatching and communication with response forces.
- joint work of dispatchers (experts) when analyzing the incident using means of collective work (video screens, remote workplaces, etc.).
- Server and telecommunication equipment should be placed in the existing server room at the address: Kyiv, str. Degtyarivska, 11G, room 312.

Composition of equipment and software Monitoring Center of the State Customs Service (hereinafter referred to as the Monitoring Subsystem), as a component of the CSP:

- **The monitoring subsystem** should be built according to the modular principle. The basic modules of the system are:
- software and technical complex of video analytics and management of a centralized database.
- software and hardware mean implementing the business logic of applied functionality, which ensures the functionality of automated workplaces (a set of certain functions, based on the tasks and powers of the role of a specialist when working with the system).
- auxiliary means.

The monitoring subsystem must be built using the "Private cloud" technology - infrastructure intended for use by fiscal and law enforcement agencies, which includes various units with different functional tasks. In the private cloud, the service model "Platform as a service" (PaaS, Platform-as-a-Service) should be implemented - a model where the consumer is allowed to use the cloud infrastructure

to host basic software for the subsequent placement of new or existing applications on it (own, custom developed or purchased replicated applications).

The monitoring subsystem should consist of the following elements:

Item	Detailed Specifications
Management servers for local video monitoring systems of international checkpoints must have technical and other characteristics per the following requirements (not less than):	• server for installation in a 19" standard cabinet. • height no more than 2U. • at least two processors, up to 28 cores per processor. • memory controllers are not less than PERC HBA. • memory not less than 24 DDR4 DIMM slots, with RDIMM / LRDIMM support, speed up to 2666 MT / s, 3TB maximum up to 12 NVDIMMs, 192 GB maximum. • storage compartments (not less than): up to 8 x 3.5" SAS / SATA HDD max. 80 TB, additional DVD-ROM, DVD + RW. • power supply no more than: 1 + 1, ≤ 495 W. • availability of ports (not less than): 4 x 1GE; front ports: video, 2 x USB 2.0, USB 3.0, rear ports: IDRAC Direct Micro-USB: video, serial, 2 x USB 3.0, iDRAC dedicated network port; video card: VGA.
Cloud system management and maintenance servers must have technical and other characteristics per the following requirements (not less than):	• server for installation in a 19" standard cabinet. • height no more than 2U. • at least two processors, up to 28 cores per processor. • memory controllers are not less than PERC HBA. • memory not less than 64 GB DDR4 DIMM, 24 DDR4 DIMM slots, with RDIMM / LRDIMM support, speed up to 2666 MT / s, 3TB maximum up to 12 NVDIMM, 192 GB maximum. • storage compartments (not less than): up to 8 x 3.5" SAS / SATA HDD max. 80 TB, additional DVD-ROM, DVD + RW. • power supply no more than: 1 + 1, ≤ 495 W. • availability of ports (not less than): 4 x 10GE; front ports: video, 2 x USB 2.0, USB 3.0, rear ports: IDRAC Direct Micro-USB: video, serial, 2 x USB 3.0, iDRAC dedicated network port; video card: VGA. • Operating systems support: Canonical® Ubuntu® LTS Citrix® XenServer® Microsoft Windows Server® with Hyper-V Red Hat® Enterprise Linux SUSE® Linux Enterprise Server VMware® ESXi. • Server must be equipped with endpoint protection and endpoint detection and response (EDR) software to safeguard against cybersecurity threats.
Streaming server	• server for installation in a 19" standard cabinet.

must have technical and other characteristics per the following requirements (not less than):	• height no more than 1U. • the processor is not worse: the number of cores is not less than 4. • memory controllers are not less than PERC HBA. • memory not less than 16 DDR4 DIMM slots, with UDIMM support, speed up to 2666 MT / s, 64 GB maximum. • storage compartments (not less than): up to 4 x 3.5" SAS / SATA. • availability of ports (not less than): 2 x 1GE; front ports: video, 1 x USB 2.0 rear ports: 2 x USB 3.0, Serial port, VGA. • Operating systems support Certify XenServsr, Citrix XenServer, Microsoft Windows Server® with Hyper-V, Red Hat® Enterprise Linux, and Ubuntu Server. • Server must be equipped with endpoint protection and endpoint detection and response (EDR) software to safeguard against cybersecurity threats.
A hard disk for storing information with a capacity of 4 TB must have technical and other characteristics per the following requirements (not less than):	• form factor: 3.5 “. • spindle rotation speed (not less than): 7200 rpm. • storage type: HDD. • capacity: at least 4000 GB. • volume of cache memory: at least 256 MB. • interface: SATA III. • data transfer speed (not less than): 190 Mb/s. • power consumption no more than 9 W.
Cloud switch must have technical and other characteristics per the following requirements (not less than):	• RAM (not worse): 2 GB. • Flash memory (not less than): 512 MB. • Ethernet ports (Uplink) (not worse): 2x QSFP+ 40Gbe; 4 x SFP+ 1000/10000 Mb/s • Ethernet ports (Downlink) (not worse): 48x RJ45 (10M / 100M / 1000M). • VLAN (not worse): IEEE 802.1Q 4096 • management (not less than): L2. • MAC table size (not less than): 128K. • power supply (not worse): 100-240 VAC • power consumption (not less than): 260W.
The router must have technical and other characteristics per	• hardware accelerated RJ-45 GE ports: 8. • hardware accelerated SFP GE slots: 8. • hardware accelerated SFP+10 GE:2 slots. • Volume of internal storage: 2 x 240 GB SSD

the following requirements (not less than):	• IPS bandwidth: 10 Gbps. • IPsec VPN bandwidth: 20 Gbps. • power supply (not worse): 100 / 240V (PSU included). • power consumption: ≤ 244W. • working temperature (not worse): 0 ° C . + 40 ° C.
The structured cable network must meet the following requirements:	• To combine the elements of the cloud platform into a single information network, it is necessary to create a structured cable network (hereinafter referred to as SCN), which must meet the following standards: • DSTU B A.2.4-40 :2009 ; • DSTU B A.2.4-42 : 2009 ; • TIA/EIA-568 A(B) Commercial Building Telecommunications Cabling "Cabling for telecommunications products and services in commercial buildings". • ISO/EIC 11801 "Information technologies. Universal cable network for the customer's buildings and territories". • TIA/EIA-862 Building Automation Systems Cabling Standard for Commercial Buildings. • EN 50173 Information technology – Generic cabling systems. • ISO/IEC TR 14763 Information technology - Implementation and operation of customer premises cabling. • TIA/EIA-942 Telecommunications Infrastructure Standard for Data Centers • BICSI Telecommunication Distribution. Methods Manual. 10th Edition: 2003 • PUE "Rules of electrical installations", • as well as meet the requirements for category 5e cable networks. • SCN must ensure: • combination of key elements of the cloud platform into a single information network. • reliability and ease of use. • speed of information transfer: 10/100/1000 Mb/s. • the possibility of expanding the system. • The topology of the SCN assembly is a "star". The number and characteristics of the component elements for the deployment of the SCN must be determined by the Contractor at the stage of the object inspection. All SCN components must be manufactured by well-known manufacturers in compliance with international quality certificates (ISO 9001, ISO 9002). For the installation (mounting) of the SCN, not less than copper symmetric cable of the "twisted pair" type, designed for data transmission using Gigabit Ethernet (1000BASE-T) category 5e

	technology, should be used. SCN should be divided into structural subsystems: a set of copper cables, switching panels, organizers, and cable connectors. The cables of the power supply network and the low-current system must be laid in separate cable channels. In workplaces and on all evacuation routes (corridors, transitions), it is mandatory to use cables whose sheath does not support the combustion process does not contain halogens, and does not emit poisonous gases in case of fire. Installation of a structured cable network must be carried out per the requirements of current standards by qualified personnel. For the passage through the walls, collateral plastic pipes should be provided, sufficient for laying the necessary number of cables, taking into account the technological reserve and meeting the requirements of the standards for the level of cable filling. In the process of preparing the cable ducts for laying the cable, the absence of sharp corners and burrs on the inner surfaces should be checked. SCN testing: - after carrying out work on the installation of SCN, all unshielded twisted pair cables are checked for compliance with category 5e cable networks for internal office premises. - testing is performed for each data transmission channel.
Telecommunication cabinet 19" the set must have technical and other characteristics per the following requirements (not worse):	• front door: with turning handle, lock, and tempered glass. • rear door: all-metal with "gill" type perforation and lock. • side walls: removable with a lock. • coating: powder coating. • cabinet design: collapsible. • class of protection against external factors: not less than IP 20. • the supporting structure is made of 1.5-2.0 mm steel (not less than). • the possibility of adjusting the distance between the rails in depth.
An uninterruptible power supply must have technical and other characteristics per the following	• number of sockets (not worse): 6 x IEC 320 C13 (battery backup power); 4 x IEC 320 C19 (battery backup). • output power (not worse): 5000 VA / 4500 W. • input voltage range when working from the mains (not less than): 160 - 275 V. • working time at full load (not worse): 4 min (4500 W). • working time at half load (not worse): 11.8 min (2250 W). • rechargeable battery: built-in.

requirements (not less than):	• impulse protection (not less than): 480 J. • type of battery used (not less than): sealed lead-acid battery with thickened electrolyte: protection against leaks. • type of architecture (not less than): continuous operation. • availability of an LCD. • battery charging time (not less than): 1.5 hours. • output voltage form: pure sinusoid.
A set of batteries for an uninterruptible power supply must have technical and other characteristics per the following requirements (not less than):	• battery output voltage (not worse): 192 V. • type of batteries: lead-acid battery. • compatibility with the uninterruptible power supply, the requirements for which are specified in clause 3.3.1.11. • expected battery life (not less than): 3-5 years. • working temperature (not worse): 0 - 40 ° C. • working range of relative humidity (not worse): 0 - 95% (without condensation).
Monitoring video camera for the monitoring room must have technical and other characteristics per the following requirements (not less than):	• the lens is not less than 1 / 3 "Progressive Scan CMOS. • maximum resolution (not less than): 2560 x 1440. • minimum sensitivity (not less than): 0.01Lux @ (F1.2, AGC on), 0.018Lux @ (F1.6, AGC on), 0 Lux with IR. • shutter speed (not less than): 1/3 s-1 / 100,000s. • support for slow shutter speed. • day/night mode (not less than): IR filter (ICR). • axis adjustment (not less than): rotation: 0 ° ~ 355 °; tilt: 0 ° ~ 75 °; rotation: 0 ° ~ 355 °. • illumination range (not worse): 30 m. • focal length (not less than): 2.8-12 mm. • lens mount: F14. • aperture (not less than): F1.6. • viewing angles (not less than): H: 98 ° ~ 28 °, V: 51 ° ~ 16 °, D: 115 ° ~ 32 °. • automatic focus control. • video compression (not exclusively but including): / H.265/ H.264 / MJPEG. • number of streams (not worse): 3 streams. • support for resolutions (not exclusively but including): 4M (2688x1520) / 3M (2304x1296) / 1080P (1920x1080) /1.3M (1280x960) / 720P (1280x720) / D1 (704x576 / 704x480) / VGA (640x480) / CIF (352x288 / 352x240). • frame rate (not exclusively but including): (mainstream) 2688 x 1520, 2304 x 1296, 1920 x 1080 - 25 k / s; Add. stream) 640 x 480, 640 x 360, 320 x 240 - 25 k / s; Addendum 2 stream: 1280 x

	720, 640 x 360, 352 x 288 - 25 k / s. • video bitrate (not worse): 32 Kbit / s - 16 Mbit / s. • noise suppression (DNR) (not worse): 3D DNR. • BLC support. • WDR (not worse): 120 db. • ROI (not less than): 1 fixed area for the mainstream and sub-streams. • image settings Rotation mode, saturation, brightness, contrast, and sharpness are adjusted by client software or web browser. • audio compression (not exclusively, but including): G.711 / G.722.1 / G.726 / MP2L2 / PCM • audio bitrate (not exclusively but including): 64Kbit / s (G.711) / 16Kbit / s (G.722.1) / 16Kbit / s (G.726) / 32-160Kbit / s (MP2L2). • Ethernet (not worse): RJ45 10M / 100M. • network protocols (not exclusively, but including): TCP / IP, ICMP, HTTP, HTTPS, FTP, DHCP, DNS, DDNS, RTP, RTSP, RTCP, PPPoE, NTP, UPnP ™, SMTP, SNMP, IGMP, 802.1X, QoS, IPv6, Bonjour. • compatibility (not exclusively, but including): ONVIF (PROFILE S, PROFILE G), ISAPI. • storage method (not exclusively, but including): NAS (NFS, SMB / CIFS), ANR, Micro SD. • browser support (not exclusively, but including): IE8 +, Chrome 31.0-44, Firefox 30.0-51, Safari 8.0+. • mobile platforms (not less than): iOS, Android. • users/levels (not worse): up to 32 users; 3 levels: administrator, operator, and user. • video interfaces (not less than): 1Vp-p (75 Ohm / BNC). • audio interfaces (not less than): 1 input / 1 output. • alarm interfaces (not less than): 1 in / 1 out. • network interfaces (not less than): 1 RJ-45 (10M / 100M). • local memory (not less than): micro-SD up to 128GB. • the presence of a reset button. • alarm triggers (not exclusively, but including): motion detection, scene change, network disconnection, IP address conflict, illegal access, storage error. • Smart functions (not exclusively but including): line crossing; invasion of the region; identification of persons. • power supply (not less than): DC 12V ± 25%. • PoE (not worse): PoE (802.3af) (Class 3). • power consumption (not worse): DC 12V: 0.8 A, 10 W; PoE: (802.3af, 37 V-57 V), 0.35A - 0.2A, max. 12 W. • working temperature (not worse): -30 ° C - + 60 ° C. • humidity: <95%. • degree of protection (not less than): IP67, IK10, TVS 2000V.

	•
Operators' working station - the PC of the operator's workplace must have technical and other characteristics per the following requirements (not less than):	• The processor is not less than than Core i7-9700F. • RAM is not less than 16 GB. • HDD is not less than 2 TB. • SSD is not worse than 240 GB. • video card not less than GTX1050Ti. • the operating system is not less than Windows 11Pro. • PCs must be equipped with endpoint protection and endpoint detection and response (EDR) software to safeguard against cybersecurity threats.
Monitor for the operator's workplace must have technical and other characteristics per the following requirements (not less than):	• screen type: TFT-LED backlight. • screen size: 24". • pixel size: no more than 0.3 x 0.3 mm. • screen resolution: not worse than 1920x1080. • brightness: at least 250 cd/m2. • contrast: not worse than 1000:1. • response time: no more than 5 ms. • viewing angle: not less than than 170/160. • interfaces (not less than): HDMI, VGA.
The keyboard + mouse set must have technical and other characteristics per the following requirements (not less than):	• interface: USB adapter 2.4 GHz. • moisture-proof keyboard. • color: black.
Type 2 uninterruptible power supply must have technical and other characteristics per the following requirements (not less than):	• number of sockets (not worse): 2. • output power (not worse): 800 VA / 480 W. • input voltage range when working from the mains (not less than): 155-275 V. • working time at half load (not less than): 10 minutes. • working time at full load (not less than): 5 min. • type of architecture (not less than): line-interactive (line-interactive). • rechargeable battery: built-in. • the type of battery used (not less than): sealed maintenance-free lead-acid battery.

	• the output voltage from the approximated sinusoid.
The network filter must have technical and other characteristics per the following requirements (not less than):	• number of sockets (not worse): 6. • maximum load current (not worse): 10 A. • cable length (not worse): 2 m. • voltage (not worse): 220 V, 50 Hz. • maximum load (not worse): 2200 W. • automatic fuse, max. (not less than): 10 A. • cable cross-section (not less than): 3x1.0 mm. • type: network filter. • filter connection type: for connection to UPS (connector C14). • presence of a switch. • availability of grounding.
Access control and management system - ACS Controller with two doors must have technical and other characteristics per the following requirements (not less than):	• processor (not less than): 32-bit high-speed processor. • number of doors: 2. • communication interface: TCP / IP. • connection interface (not less than): RS-485, Wiegand. • memory (not worse): maps: 100,000; events: 300,000. • status indication (not less than): power supply status, communication status, working status. • wall reader (not less than): via Wiegand (4 readers) or RS485 (up to 4 readers). • input interfaces (not less than): 13 (2 - door sensors, 4 - alarms, 4 - input, 2 - exit buttons, 1 - unauthorized access). • output interfaces (not less than): 2 relay outputs, 4 - alarms. • power consumption ≤100 W. • working temperature (not less than): -20 ° C - +65 ° C.
The battery must have technical and other characteristics per the following requirements (not less than):	• type (not less than): AGM technology. • capacity (not less than): 7Ah. • voltage (not less than): 12V.
Terminal with face and fingerprint recognition function must have technical and other characteristics per the following	• operating system: Linux. • camera (not less than): two 2MP each. • the memory of maps and events (not worse): 6,000 maps, 50,000 events. • finger memory (not worse): 5000 fingerprints. • the memory of persons (not worse): 6000 persons. • presence of fingerprint comparison mode. • card reading delay (not less than): <1 s. • delay in reading faces (not less than): <0.2 s.

requirements (not less than):	• card type: Mifare. • modes of operation: recognition of persons. • reading distance (not less than): 3 m. • the communication interface (not less than): 1x RJ45 (10M/100M). • input interfaces (not less than): 1x USB, 1x RS-485, 2x alarm input. • output interfaces (not less than): 1x lock, 1x door sensor, 1x exit button, 1x alarm output. • display (not less than): 7-inch touch screen. • power supply (not worse): DC 12V / 2A, 24 W. • working temperature (not less than): from -30 to +60 ° C. • humidity (not less than): from 0 to 90%. • degree of protection (not less than): IP65. • availability of anti-sabotage function.
The exit button for the server room must have technical and other characteristics per the following requirements (not less than):	• device type: exit button. • dimensions (no more): 83x32x25mm. • material: stainless steel. • nominal current (not less than): DC12V. • output interfaces (not less than): NO / COM.
The electromagnetic lock must have technical and other characteristics per the following requirements (not less than):	• device type: electromagnetic lock. • place of installation: premises. • installation type: overhead. • holding power (not less than): 280 kg. • the presence of a door status sensor. • indication: light. • supply voltage/power source: DC 12V / DC 24V. • consumption current (not worse): 500/250 mA. • material (not less than): anodized aluminum (lock) | zinc (bar). • working temperature (not less than): -10 ~ +55 ° C.
Puller must have technical and other characteristics per the following requirements (not less than):	• device type: door closer. • door weight (not worse): 120 kg. • door width: maximum 950-1400 mm. • type of lever. • door opening angle (not worse): from 80 ° to 180 °. • the possibility of adjusting work modes. • color: silver. • Operational temperature (not worse): from -30° C to +50 ° C.
The magnetic contact detector must have	n/a

standard technical and other characteristics according to the purpose.	
The terminal for working with fingerprints must have technical and other characteristics per the following requirements (not less than):	• device type: fingerprint input device. • communication interface (not less than): USB 2.0. • availability of state indication. • output interfaces (not less than): USB 2.0. • power supply (not worse): 5 VDC, 200mA. • working temperature (not worse): -30 ° C to + 70 ° C. • size (no more): 100mm x 48mm x 35mm. • color: black.
The terminal for working with cards must have technical and other characteristics per the following requirements (not less than)- device type:	• USB card input device. • communication interface: USB 2.0. • frequency response: 13.56MHz and 125KHz. • availability of state indication. • output interfaces: USB. • power supply: USB. • power consumption (not worse): 200mA. • working temperature (not less than): -20 ° C ~ +65 ° C. • size (no more): 117mm x 67.5mm x 14.3mm. • color: black.
Assembly set - the type and dimensions of the installation kit are specified at the stage of the inspection of the ACS installation facilities, and preliminarily consist of the following parts:	• set of connectors: 1 set. • a set of consumables (screws, bolts, self-tapping screws, dowels, drills, etc.).

ANNEXES

ANNEX 1 - EXAMPLE LIST OF USER ROLES AND FUNCTIONS

Position	Functions and available Roles in the system
Security Admin	Access to these functions is provided through the interface of ITMS/CIIP: - Creation of users (operators) in the system. - System access rights management. - Logs viewing. - Viewing the log of actions both for a certain time and for a particular user in the system. - History of own activities.
Administrator – Moderator	Access to these functions is provided through the interface of ITMS/CIIP: - Setting up a transport management system in the pilot road BCP between controlled areas. - Access to the settings page, where it will be possible to create new alarms and edit existing ones. - Theme customization. - History of own activities.
Customs Officer – Procedure monitoring	Access to these functions is provided through the interface of ITMS/CIIP: - Access to the search page. - Ability to search in the system for information about border crossings by both driver's surname and vehicle registration number. - Real-time video monitoring of vehicles within the pilot BCPs territory using license plate numbers or driver's surnames as a means of recognition. - Urgent search of information about the location of vehicles within the pilot BCP using license plate numbers or driver's surnames as a means of recognition. - Case analysis in real-time mode and by analyzing archives. - Access to basic information regarding border crossings by specific individuals and vehicles. - Interface for generating reports for a specific period, both for all controlled territories and individual ones. - History of own activities. Please note! This position is not authorized to make any changes in ITMS/CIIP systems.
Customs Officer – Performance	Access to these functions is provided through the interface of ITMS/CIIP: - Access to the page with performance indicators of BCPs operations.

monitoring	- Real-time video monitoring of vehicles within the pilot BCPs territory using license plate numbers or driver's surnames as a means of recognition. - Case analysis in real-time mode and by analyzing archives.
Customs Officer – An authorized representative of Customs with the right to review all information	Access to these functions is provided through the interface of ITMS/CIIP: - Ability to search the information in the system for border crossing using license plate numbers or driver's surnames as a means of recognition. - Access to full information regarding border crossings by specific individuals and vehicles. - Access to a page displaying BCPs performance indicators. - Viewing data on vehicles with specific risk profiles. - Review of data on vehicles with wanted license plates. - Applied alarm settings. - List of connected equipment for each checkpoint. - History of generated requests. - Interface for generating reports for a specific period both for all and for certain BCPs. - Viewing logs and all actions of operators. - History of own activities. Please note! This position is not authorized to make any changes in ITMS/CIIP systems.

ANNEX 2 - EXAMPLE OF CONTROL PROCEDURES

№	Area of BCP	Time (formed automatically)		Results/decision	Decision maker	Note	Who watches
		start	start				
1	2	3		4	5	6	7
1.	Entry to BCP						
2.	Stay in the waiting area for customs clearance						
3.	Border control						
	Second-line control						
4	Customs control						
	Control procedures in the zone of advanced control: scanner, tow yard, box						
	Completion of customs control after procedures in the advanced control zone						
5.	Stay in the waiting area for exit from BCP						
6	Exit from BCP						

Example of an algorithm of control procedures at the “Exit from Ukraine” passenger direction.

1. Passing customs and border control without objections.
2. Return of vehicle from any area of BCP to the customs territory of Ukraine.
3. Customs/border services send the vehicle to the Enhanced Control Zone/for second-line control from Area 2.1. and return to the customs territory of Ukraine.
4. Customs/border services send the vehicle to the Enhanced Control Zone/for second-line control from Area 2.1. Permission and moving to the territory of the bordering state.
5. Delivery to the Customs warehouse at the BCP (export zone)
6. Delivery to the Customs warehouse beyond the BCP

Example of an algorithm of control procedures at the “Exit from Ukraine” cargo direction.

1. Passing customs and border control without objections.
2. Return of vehicle from any area of BCP to the customs territory of Ukraine.
3. Scanning the vehicle, customs clearance, and border crossing.
4. Scanning the vehicle, the vehicle returns to the customs territory of Ukraine.
5. Transfer of temporarily detained vehicles to the tow yard based on the results of control procedures preceding customs clearance, customs clearance, and border crossing.
6. Transportation of oversized cargo

Example of e-ticket

E-TICKET (exit passenger direction)

Automatically formed information.

Direction of movement: Exit from Ukraine
Shift on duty: «21.00» «__»/ «09.00» «__» _____20__, nighttime; or «___» _____ 20__, daytime.
Date and time of entry:
Note for "Other movements": "О", "Д", "М."
Lane: red/green corridor.
Registry number of the vehicle
Registry country of the vehicle
Registry number of the trailer (semi-trailer, home on wheels, etc.)
Registry country of the trailer,
Photograph of the vehicle made by license plate recognition system.

Information was filled in by the border guard officer.

Additional stamp placed in the terminal: number of passengers.

(***There must be a slot to fill in the original data and the data that have changed during the control procedures).***

Additional stamp placed in the terminal by the border guard officer: diplomat (in case such person is in the vehicle).

Control ticket (visualization).

№	Area of BCP	Time (formed automatically)		Result/decision	Decision maker	Note*
		start	finish			
1	2	3		4	5	6
1.	Entry into BCP					
2.	Stay in the waiting area for clearance					
3.	Border control					

4.	Customs control					
5.	Stay in the waiting area for exit from BCP					
6	Exit from BCP					

***** Note:

- return stamp must be placed in the column that corresponds to the stage when the decision was made.

- “O” stamp must be placed for “Service” (for example, bank, café, Data-Group, etc.).

- The «МБТ» stamp stands for a vehicle that transports the goods to a Duty-Free Shop (“МБТ”) located in BCP