Comments by Economic Operator 1

“Integrated Digital System for Managing Electronic & Physical Security with the Provision of Security and Fire Safety Services at the Facilities of EYDAP SA”

General Proposal:

The system/project under design is multi-layered and particularly demanding, as it includes both an Access Control System in combination with a Surveillance System. Consequently, it must be of high quality and top performance.

You may have already foreseen the need for quality evaluation, which means assessment/scoring based on qualitative and proven criteria (with certifications, etc.). If you have not yet considered this, then you need to examine this possibility.

Our company has been active in this field for 30 years. We have witnessed many implementations of such systems stagnate immediately after installation. This has been due to:

- the quality of construction,
- the construction culture,
- and whether the systems are mere copies.

As a result, the implementation and use of such systems becomes compromised, leading users to disappointment and ultimately to abandonment of the original idea.

We understand that today the EU and our country impose restrictions only on products of Russian possibly also Iranian origin. Therefore, the only solution is to define qualitative criteria and their scoring, so that a mathematical evaluation/scoring formula can be derived.

1. **CCTV**

1.1 / 1.2

It should be allowed to propose the combination, during installation, of a separate thermal and optical camera — that is, two distinct cameras, possibly from different manufacturers as long as they are operational within the same management system.

1.18 / 1.19 / 1.20

We propose that the analog cameras be replaced with IP cameras. Most manufacturers have discontinued their production. More importantly, IP cameras are significantly more user-friendly, functional, based on modern technology, and much more flexible in terms of support.

3. Access Control System

3.1

The controller's metal enclosure restricts competition. If for any reason you consider it absolutely necessary, then the integration of the controller into a metal box should be allowed, with or without its power supply unit.

3.2

It should be specified that the card reader must support the following capabilities:

- RFID technology
- NFC (which allows the use of mobile phones as a unique credential tool — currently free for Android devices and subscription-based per user annually for Apple phones)
- Bluetooth Low Energy (BLE) which allows the use of all mobile phones without a subscription.

If you intend to integrate visitor management into the overall system, then you may need to define the visitor control/reception points per building. Corresponding readers at these points should, in addition to the above features, also support **QR-code reading**.

The Software should thus support visitor management functionalities such as:

- invitation via email,
- entry of ID details,
- vehicle license plate number,
- QR-code generation and delivery, etc.

3.11/ 3.12

The use of a UHF antenna with a range of 7–10 meters is recommended to detect an adhesive label on the vehicle's windshield. This avoids the need for a special combi card (UHF & RFID), which is four times more expensive when combined with RFID technology. It also avoids the need for a second UHF card that would remain in the vehicle while the driver carries another card to access work areas.

If you want the employee to have the flexibility to switch vehicles, then either: a second UHF adhesive label must be issued, or the antenna should be replaced with an ANPR (Automatic Number Plate Recognition) camera, allowing users to register two or more license plate numbers.

However, the latter solution does not accommodate motorcycle owners, which further supports the use of UHF adhesive labels, as there are specially reinforced adhesive labels designed for installation on the motorcycle headlight (with different cost than the standard label intended for vehicle windshields).

6. Electronic Key Management System

We would like to bring to your attention the following technology, which we can also demonstrate at your premises:

For preventive maintenance and corrective interventions by technicians, we propose a Keyless Access Control System operating via cloud computing, which will provide unlimited flexibility and immediacy in managing technician/employee visits always under full control and audit trail.

This eliminates the need for managing physical keys, which is not only time-consuming but also cost-intensive.

General Requirements

- Online virtual key system, with no physical/mechanical key, no card, no electronic keypad, etc.
- Special locks that recognize virtual keys.
- Padlock for outdoor use on the station's main gate (fence gate) and on the shelter door.
- The padlocks must:

    - operate through a real-time management system,
    - report their locked/unlocked status to the Coordination Center in real time,
    - be independent of electrical power and network infrastructure.
- The battery life of padlocks must exceed 7 years with one unlock operation per day.

The Padlock:

- Must be vandal-resistant and durable under stress, with no keyhole, no keypad, and no exposed power contacts.
- Must be highly resistant to extreme weather conditions and harsh environments, with a minimum protection rating of IP66.
- Must remain corrosion-free for at least 10 years.
- Must comply with the following certifications, or equivalent:
    - Impact protection: IK10 according to EN 62262
    - Sealing requirement: IP66
    - Impact resistance: EN 12320 – Grade 6
    - Drop test: according to IEC 60721-4-2 (IEC 60068-2-32), class 2M3
    - Mechanical shock: according to IEC 60721-4-5, class 5M3
    - ESD (Electrostatic Discharge): EN 61000-6-2 (X3 of the standard)
    - Vibration: IEC 60721-4-5:2001+A1:03 (IEC 60068-2-64), category 5M – minimum 500
    - Must have a holding force of at least 5,000 kg.

Virtual Key Access Control Software

The software will be installed on the central server of the Coordination Center (CC) and will allow full real-time management, with the following functions and capabilities:

- Establishment of a virtual key via an application for smart devices such as mobile phones and tablets,
- Opening authorizations will be granted through a secure application (with two-factor authentication),

- The management system must offer a cloud-based solution on the CC's infrastructure,
- Access authorization: an authorized mobile phone receives permissions to open a specific lock at a specific geographic location, for a specific period and number/duration of openings,
- Virtual key protection: access to the mobile application requires a username,
- Authorization rights are issued by a management system, based on the access rules defined by the provider,
- Fingerprint unlocking: the lock can be configured to unlock via fingerprint recognition through the user's app,
- Real-time alerts: the management system must be capable of sending automated notifications (via SMS and/or email) to designated recipients based on predefined real-time events, such as abnormal access requests, emergencies, etc.,
- Geo-fencing capabilities: the system must be able to allow or deny access to padlocks or locks based on geographical boundaries,
- The management system must provide API integration with other systems, such as access control, HR management, ERP, CRM, etc.

Cybersecurity of the Virtual Key System

- The system must be protected by multi-layer encryption, with a minimum of 256-bit asymmetric encryption, both for data and secure communication channels.
- Decryption must occur only on the server and at the lock, with no decryption of data on the mobile application.

12. Pilot Operation Phase

It is proposed that Pilot Operation be included in Section 12.

After the installation is completed, the Contractor must place the installed systems into Pilot Operation under real conditions for a period of two months, starting from the system installation date.

During the Pilot Operation period, the Contractor will have the following obligations:

- Support to the Contracting Authority in the operation of the proposed systems/applications.
- Final functional tests, additions and modifications, integration and trial use of systems and applications, aiming to verify proper functionality and smooth interoperability.
- Improvements to the proposed systems/applications.
- Problem resolution.
- Error correction and management.
- User support with the physical presence of the Contractor's staff, e.g., collecting user feedback, assisting in handling and operating applications and equipment, etc.
- Operation and support of a Help Desk system.
- Documentation updates.
- On-the-job user support.
- Maintenance of equipment, software, and applications.

The following must be completed during the Pilot Operation period:

- Configuration, customization, and adjustments of the system software.
- Full integration of the proposed systems and applications.
- System tuning for performance optimization (fine-tuning).

If, during the Pilot Operation period, problems arise or it is determined that some of the specified requirements are not met, the Contractor is obliged to promptly implement the necessary corrective actions and adjustments so that, by the end of the Pilot Operation period, the system is ready for productive deployment and operation.
Any problems that may arise during the Pilot Operation must be appropriately addressed by the Contractor before the project is completed.

13. In addition to all points mentioned in this section, we also propose the following, based on our experience to date:

Remote Monitoring & Supervision

Uninterrupted remote monitoring and supervision of the entire system's operation (hardware, software, network equipment, etc.) using appropriate surveillance systems.

Fault Reception Center

24/7 operation for the entire duration of the contract, staffed by technicians specialized in providing technical guidance for the resolution of minor issues.

Preventive Maintenance

Preventive maintenance in accordance with a plan that must be included in the technical offer. The plan should provide for at least two interventions per year.

As part of the preventive maintenance activities, the Contractor is obliged to inspect the proper functioning of all installed devices, including sensors, optical and thermal cameras of the detection system, CCTV systems, cabling, junction boxes, connection cables and surge protection devices, uninterruptible power supply (UPS) units, and all components that make up the peripheral units, according to the general indicative checks listed below:

- Inspection of the power supply system, including the main supply system, verifying the effectiveness of protection devices (circuit breakers, fuses, etc.) and any backup batteries/UPS.
- Mechanical adjustment of all cameras and sensors, as well as all components.
- Inspection of the proper operation of peripheral stations, especially transceiver equipment and antennas.
- Thorough cleaning of the external parts of sensors and camera lenses.
- Verification of the correct functioning of the cameras.
- Verification of the proper operation of installed hardware and software.
- Inspection of the overall condition of the installation.

Similarly, the above-mentioned indicative inspections must also be carried out on the Wi-Fi transmission systems (if used), including the condition and alignment of antennas, cables, and all related infrastructure.

All components found to be malfunctioning must be repaired or replaced with suitable spare parts of equal or superior specifications.

Upon completion of the work, a detailed report must always be issued, specifying, for each station, the tasks performed and the corresponding results.

Field Calibration

Verification of measurements must be carried out every six months (in alignment with the above preventive maintenance schedule). The calibration of each sensor must be checked, and written confirmation must be provided. Calibration must be performed in accordance with the criteria and methods defined by the relevant standards and/or procedures.

Corrective Maintenance

Corrective maintenance will, in most cases, be carried out through the replacement of units or sensors. The Contractor must ensure the availability of spare parts and consumables in sufficient quantities and geographically distributed according to the installation areas, in order to guarantee the availability of the entire system covered by the contract, as specified in these technical specifications.

The Contractor must specify in their proposal the locations where spare parts will be stored, ensuring compliance with the required response and system restoration times.

Interventions, without any limitation on the number or type, will include the supply of spare parts and consumables necessary for restoring proper system functionality. These will be carried out in a way that optimizes restoration time, including the replacement of individual units (e.g., sensors, electronic boards, modules, and functional components), which may subsequently be repaired by the awarded contractor and reused for future corrective maintenance services.

Corrective maintenance must be initiated:

- Upon specific notification from the Contracting Authority, which, to the extent possible and based on the available information, will indicate the type of malfunction. This report will be sent via a dedicated electronic message to the Technical Director of the Contractor, who will be designated for this purpose at the time the contract is signed.
- By the Contractor, based on periodic inspections conducted both on-site and with the assistance of remote technical verification tools. In this case, the Contractor’s Technical Director is obliged to inform the Technical Director of the Contracting Authority of the identified malfunctions and the proposed intervention schedule.

Remote Diagnostics and Remote Control

For maintenance purposes, various remote access methods are foreseen for monitoring the operation of on-site instruments. The Contractor will receive the operational plan of the monitoring and control system for the management of wireless communication and GSM/GPRS/UMTS modems, as well as the instruments and data transmission systems. In addition, a designated user will be granted access to the Control Center's monitoring system.

With this tool, it will be possible, for example, to:

- monitor the status and progress of maintained instruments,
- check the operational status of cameras and management/storage servers,
- identify cameras or sensors that are not transmitting data properly.

If the software owned by the Contracting Authority is not suitable for remote connection to the equipment installed at the data collection stations, the Contractor must provide the necessary application, along with the appropriate user license allowing its use.

It is understood that the Contractor must be able to access the remote diagnostic tools, regardless of the infrastructure of the Control Center. The Contracting Authority will guarantee access to a dedicated station, either remotely or on-site, based on its own security policies.

Intervention Time

Regarding the Service Level Agreement (SLA) for maintenance services, the definitions of Critical, Major, and Minor Failures are used, as described below. The Contracting Authority is solely responsible for classifying each failure as Critical, Major, or Minor.

For corrective maintenance services:

- Response Time is defined as the time interval from the notification of the fault or the creation of a service request by the Contracting Authority to the Contractor (either via telephone to a designated representative of the Contractor or via email or other electronic application), until the arrival of Contractor personnel (or their authorized representatives) at the fault location or until the Contractor informs the Contracting Authority that the issue is under investigation.

- Resolution Time is defined as the time from the fault notification until the moment of final resolution of the issue or, if not feasible, its temporary mitigation, following prior notification and approval by the Contracting Authority.

The Contractor is obligated to comply with the following Response and Resolution Times for each failure category:

Failure Category	Response Time	Resolution Time
Critical	2 hours	4 hours
Major	4 hours	8 hours
Minor	12 hours	48 hours

For all sites where access must be secured by the Contracting Authority for the Contractor's personnel, the times above start counting from the moment access is granted. In cases of catastrophic events or inaccessibility of certain locations, the intervention times may be adjusted by the Contracting Authority.

In addition to the two-year SLA-based operational support and warranty period, all hardware and software must be covered by the manufacturer’s warranty, if it exceeds the two years specified in the contract with the Contractor.

Excluded Interventions

The following causes are excluded from the scope of corrective maintenance interventions:

- Acts of vandalism
- Lightning strikes resulting in total system component failure
- Extreme natural phenomena such as floods, deluges, earthquakes, avalanches, or landslides
- Theft

Comments by Economic Operator 2

1. Communication Network

EYDAP (Athens Water Supply and Sewerage Company) constitutes critical infrastructure for Greece, as it ensures the uninterrupted supply of clean and safe water to millions of citizens in Attica, the most populous region in the country. Its role is fundamental to social well-being, economic activity, and national security, since any disruption in its operation would have serious consequences for citizens' daily lives, the operation of critical facilities, and the response to emergency situations.

For this reason, we believe that the Communication Network equipment must meet certain minimum standards in terms of security, quality, operational functionality, and business continuity.

The points to be covered with networking equipment are as follows:

- 2 sites: Command & Control Centers (C&CC) of Systems
- 9 sites/facilities:
    - 4 x Water Treatment Units (WTU)

    - 5 x Wastewater Treatment Plants (WWTP)
- 31 sites: Offices – Cash Service Points
- 275 aqueduct sites, including:
    - 13 x Dams, Hydroelectric Plants (HPP), Local Management Units (LMU), or Pumping Stations
    - 5 x Type-L Flow Regulators
    - 70 x Sewerage Pumping Stations
    - 141 x Water Supply Points (Pumping Stations or Reservoirs)
    - 46 x Cathodic Protection Points

Clarifications and Technical Requirements per Category

1.1 Field Network Equipment

Questions:

- Does the Field Network Equipment concern the 275 points as described above? Or which specific points does it refer to?
- How many and which of these points will be interconnected via a ring topology, using single-mode fiber optic connections?
- How many RJ-45 ports are required for the interconnection of cameras, loudspeakers, etc., and how many watts per port are needed on the switch to supply power through Power over Ethernet (PoE)?
- Will the network equipment installed in pillars require a specific protection class (e.g., IP30)?

Comments:

- Must support integrated primary and backup power supply (220V AC).
- Power consumption under full load (without PoE) must be ≤ 200 Watts.
- Support for IEEE 802.1AE MACSec-256 on all offered ports.
- Support for mechanisms to prevent execution of modified/malicious software during switch boot-up.

- Support for the runtime detection of modified/malicious software.
- Support for protection against tampering attempts on software during operation.
- Support for software-based validation of switch hardware authenticity and integrity.
- Support for encrypted storage of keys, passwords, and access certificates.
- Capability for DIN rail mounting.
- Industrial grade build suitable for harsh environments, with at least IP30 rating, fanless and without moving parts, and resistance to:
    - Temperature ranges from -40°C to +75°C
    - Vibrations, shocks, power surges, and electrical noise

It is important to know:

- How many points will this equipment be deployed at, and
- How many users will be present at each point (including systems, terminals, wireless access points, or any other device connected to the network etc).

1.2 Peripheral Network Equipment

Questions:

- Which of the above-mentioned sites (Chapter 1: Communication Network) does the Peripheral Network Equipment apply to?
- How many and which of these sites will be connected via a ring topology using single-mode fiber optic cabling?
- How many RJ-45 ports are required to connect cameras, loudspeakers, etc., and how many watts per port are needed on the switch through Power over Ethernet (PoE) to power these devices?
- Does the network equipment require a specific protection class (e.g., IP30)?

Comments:

- Support for stacking with a minimum stacking bandwidth of ≥ 480 Gbps
- Support for a minimum of 8 switches per stack
- Compact mechanical design, requiring 1 rack unit (1 RU) of space
- Support for primary and backup cooling fans

- Support for integrated primary and redundant power supply (220V AC)
- Maximum power consumption at full load (without PoE): ≤ 200 Watts
- Support for IEEE 802.1AE MACSec-256 on all offered ports
- Support for a mechanism to prevent the execution of modified/malicious software during switch startup.
- Support for checking the execution of modified/malicious software during switch operation.
- Support for checking malicious attempts to tamper with the software during switch operation.
- Support for checking by the software that the switch hardware is authentic and unmodified.
- Support for encrypted storage of keys, codes and access certificates. Support for encrypted storage of keys, passwords, and access certificates

It is important to know:

- How many sites is this equipment intended for, and
- How many users or devices will be present at each site (including systems, terminals, wireless access points, and any other network-connected elements etc).

1.3 Core Network Equipment

Questions:

- Which of the previously mentioned sites (Chapter 1: Communication Network) does the Core Network Equipment apply to?
- How many RJ-45 ports are required for the interconnection of users/systems, and how many watts per port are needed on the switch via Power over Ethernet (PoE) to power the connected devices?

Comments:

- Support for stacking, with a minimum stacking bandwidth ≥ 480 Gbps
- Support for at least 8 switches per stack
- Compact mechanical design with a 1 rack unit (1 RU) space requirement
- Support for primary and redundant cooling fans
- Support for integrated primary and backup power supply (220V AC)

- Power consumption at full load (excluding PoE): ≤ 200 Watts
- Support for IEEE 802.1AE MACSec-256 on all offered ports
- Support for mechanisms to:
    - Prevent the execution of modified/malicious firmware during switch boot-up
    - Detect the execution of malicious software during normal operation
    - Block tampering attempts during operation
    - Verify hardware authenticity (that the switch is genuine and unaltered)
- Support for encrypted storage of keys, passwords, and access certificates

It is important to know:

- How many sites this equipment concerns, and
- How many users are present at each site (including systems, terminals, wireless access points, or any device connected to the network etc).

1.4 C&CC Network Equipment

Questions:

- Does the C&CC Network Equipment apply to the two sites described above?

Observations / Comments:

- Support for stacking with a minimum stacking bandwidth of ≥ 480 Gbps
- Support for at least 8 switches in a stack
- Compact mechanical design, requiring 1 rack unit (1 RU) of space
- Support for primary and backup cooling fans
- Support for integrated primary and backup power supply (220V AC)
- Power consumption at full load (without PoE) must be ≤ 200 Watts
- Support for IEEE 802.1AE MACSec-256 on all offered ports
- Support for mechanisms to:
    - Prevent execution of modified/malicious firmware during switch startup
    - Detect modified/malicious software during operation
    - Prevent malicious tampering attempts during operation
    - Verify hardware authenticity ensuring the switch is genuine and unaltered
- Support for encrypted storage of keys, passwords, and access certificates

It is important to identify:

- How many sites this equipment will serve, and
- How many users/systems/devices will be located at each site (including terminals, wireless access points, and any other network-connected components etc).

1.5 Media Converters

If needed, the required quantity will be procured accordingly for use.

1.6 Network Equipment Installation Accessories

Depending on the number of sites and users/systems, the corresponding UTP and fiber optic cables will be provided.

1.7 Firewall Equipment for Network Protection of Facilities

Questions:

- What is the number of firewalls required per site?
- How many users will be served per site by the firewall(s)?
- Will specific security policies (e.g., web filtering and antispam) be implemented?
- Is there a defined number of VLANs, or will that be determined during the design phase with your engineers?

Comments:

- The proposed firewalls must be centrally managed by a unified management system installed on-premises, either as a virtual machine (VM) or as a vendor-supplied appliance.
- The proposed firewalls must be able to detect and block malicious software in encrypted traffic without decrypting the encrypted channel.
- They must also be able to detect Layer 7 (L7) applications in encrypted traffic without decrypting the channel and enforce application control policies.
- The proposed firewall solution must allow easy API integration with a DNS security solution from the same vendor for extended DNS protection.
- It must support an Intrusion Prevention System (IPS) engine based on machine learning for detecting and blocking malicious activity.

- The solution should support an AI assistant, integrated via the cloud with the on-premises firewall management system, offering AI-based capabilities such as:
    - Policy optimization
    - Configuration guidance (interactive dialogue with AI agent for configuration and troubleshooting of the firewalls)
- The proposed VPN agent should be unified and integrate with other vendor solutions (e.g., SSE and DNS security), ensuring that remote users remain protected even when not connected to the VPN, and allowing future implementation of content filtering policies even without VPN connectivity. These additional vendor solutions (e.g., SSE, DNS security) should not be part of the current tender.
- The proposed firewalls must be future-compatible with NAC solutions (Network Access Control), enabling enhanced profile-based access control prior to VPN access, and should support unified segmentation policies across campus, data center, WAN, and cloud security solutions, based on TAGs.

It is essential to know:

- How many sites are covered by this firewall solution, and
- How many users, systems, terminals, wireless access points, or other network-connected devices are located at each site etc.

1.8 Firewall Equipment for Network Protection (C&CC)

Questions:

- What is the number of firewalls required per site?
- How many users will be served per site by the firewall(s)?
- Will security policies be implemented (e.g., web filtering and antispam)?
- Is there a specific number of VLANs required, or will this be defined during the design phase with your engineers?

Comments:

- The proposed firewalls must be managed centrally by a unified management system installed on-premises, either as a virtual machine (VM) or a vendor-provided appliance.

- The firewalls must be able to detect and block malicious software in encrypted communications without decrypting the encrypted channel.
- They must also detect Layer 7 (L7) applications in encrypted traffic without decrypting it and enforce application control policies.
- The firewall solution must support simple API integration with a DNS security solution from the same vendor to enable extended DNS protection.
- The firewall must support an IPS engine based on machine learning, for malicious activity detection and prevention.
- The solution should support a cloud-connected AI assistant integrated with the on-site firewall management system, offering AI-based capabilities such as:
    - Policy optimization
    - Interactive configuration guidance via a dialog with the AI agent, assisting with setup and troubleshooting
- The VPN agent must be unified and integrated with other vendor solutions (e.g., SSE, DNS security), ensuring that remote users remain protected even when not connected to the VPN, and enabling the application of content filtering policies in the future, even without VPN connectivity.

Note: Other vendor solutions such as SSE and DNS security should not be offered in this tender.

- The proposed firewalls must also be future-compatible with NAC solutions, enabling profile-based access control before VPN access, and must support unified segmentation policies across campus, data center, WAN, and cloud security environments, based on TAGs.

It is essential to know:

- How many sites will this firewall equipment cover, and
- How many users, systems, terminals, wireless access points, or other network-connected devices are present at each site.

1.9 5G Cellular Router

Comments:

- In locations without fixed internet connectivity, a router/firewall capable of accepting 5G SIM cards may be offered.
- How many ports are required on the router/firewall?
- Power consumption at full load (excluding PoE) must be ≤ 200 Watts.
- Support for a mechanism to prevent the execution of modified/malicious software during router boot-up.
- Support for detection of modified/malicious software during router operation.
- Support for protection against malicious software tampering during router operation.
- Support for software-based verification that the router's hardware is authentic and unmodified.
- Support for encrypted storage of keys, passwords, and access certificates.
- Support for Software-Defined WAN (SD-WAN) capabilities for high availability, scalability, and simplified deployment.
- Support for multiple cellular technologies (5G, 4G LTE, 3G, and 2G) to ensure the best available connection.
- DIN rail mounting capability.
- Support for serial communication protocols, such as SCADA, DNP3, T101-104, Raw Socket TCP and UDP.
- Modular architecture to allow port expansion within the same router/switch unit.
- Industrial-grade design suitable for harsh environments, with at least IP30 rating, and:
    - No fans or moving parts
    - Resistance to temperatures from -40°C to +75°C
    - Protection against vibration, shock, power surges, and electrical noise

1.10 Mobile Telecommunications Subscriptions

Comments:

- It is not clear whether the required APN configuration refers solely to the two (2) Command & Control Centers or also to additional sites.
- The requirements and needs for the APN are not clearly defined, particularly whether a Dedicated APN with IPSec is required.
- Given the possibility of insufficient mobile signal coverage, Starlink satellite internet connectivity should be mentioned as an alternative solution.
- The required monthly data volume per SIM card must be specified.

1.11 Telecommunication Subscriptions for Large Facilities

Comments:

- In case the communication link cannot be implemented via LMDS, the use of fiber optic connectivity should be specified as an alternative solution.

1.12 Telecommunication Subscriptions for Command & Control Centers (C&CC)

Comments:

- It is not clear whether the switching from the primary communication link (1Gbps fiber optic) to the backup link (1Gbps LMDS) will be the responsibility of the Contractor or EYDAP.
- In the event that the backup link cannot be implemented via LMDS, the use of fiber optic connectivity as an alternative must be specified, ensuring it follows a physically diverse end-to-end route from the primary link.
- It is also unclear whether there is a specific requirement for monthly service availability expressed as a percentage.

1.13 Additional Observations / Proposed Architecture

For each site, depending on its user/system load, the proposed design is as follows:

1. Firewalls, where high availability is required per site, acting as:
    - A security perimeter/firewall enforcing the appropriate policies, protecting users and systems
    - A router connected to the telecommunications provider's router
    - Support for SD-WAN functionality
2. Firewall/Router/Extender with 5G connectivity, to be used at remote sites where a fixed line is not available.
3. Interconnection of the above devices with two central high-speed switches, ideally with 10G fiber optic capability, to ensure high availability (distribution layer) where required, e.g., at central locations such as the C&CC.
4. At sites with fewer users, where central switches may not be necessary, lower-capacity switches will be used.
5. Provision of wireless network access, depending on user load — for example, at Offices – Cash Desks via Access Points, which will be placed appropriately following a wireless design conducted by certified engineers using certified software tools (e.g., Ekahau). Different wireless network segments will be available for staff and guest access (e.g., internet access).
6. Network infrastructure security will be enforced through a Zero Trust architecture, where each user/system connected to the network is continuously monitored to ensure that any attack is mitigated — e.g., protection against rogue access points or man-in-the-middle attacks.
7. Appropriate VLAN segmentation of the network will be applied, primarily to enhance security.
8. Provision of installation and appropriate configuration services for the entire network equipment.
9. Ongoing support from the network equipment partner, covering:
    - Hardware replacement in case of failure
    - Policy changes
    - Configuration adjustments

10. Optionally, FTTO (Fiber to the Office) technology may be offered within buildings, providing high-speed connectivity (e.g., 2.5 Gbps or 5 Gbps) per wireless Access Point (WiFi 6 or WiFi 7).

Important Notes:

- The proposed architecture above is entirely indicative and will dynamically adapt depending mainly on the number of users/systems to be supported.

2. Cameras

Due to the critical nature of the infrastructure, it is recommended that all cameras carry, at a minimum, NDAA certification.

Comments by Economic Operator 3

Comments within the context of the consultation on the tender document regarding the installation of the “Integrated Digital System for the Management of Electronic & Physical

Security with the provision of Security and Fire Safety Services at the facilities of EYDAP SA".

Dear Sirs,

Following the submission to the company's responsible parties of the tender document concerning the installation of the "Integrated Digital System for the Management of Electronic & Physical Security with the Provision of Security and Fire Safety Services at the Facilities of E.YD.A.P. S.A.," we hereby communicate through this letter our observations and concerns regarding the design and implementation of the project.

As has been proven many times in the past, our company's main concern is the functionality of the proposed solutions, both in terms of operation and business performance.

The points of the tender document that, in our opinion, require attention are the following:

a. The integration of equipment from different manufacturers and sub-suppliers, which affects the proper operation of the security system in the facilities of E.YD.A.P. S.A., if the document imposes the provision of a single supplier, making it impossible for the same company to conduct an integrated study. Even in the case where a group of companies participates in the competition, there would be conflicting interests, resulting in competition rather than cost reduction for the overall project implementation. A possible separation of the categories and simultaneous definition of the budget (price ceiling) for each category separately would result in many financial benefits for the Organization, given that all participating companies would "submit much lower cost offers."

b. The absence of a central implementation and installation study, under the responsibility of the Organization, essentially imposes on the companies participating in the competition to present their own studies, resulting in the inability to conduct a uniform evaluation both at a technical and economic level. This lack of specific criteria, especially at a time when each party will present their own solution with "their own logic," and the definition by the Organization of a centralized study that will include not only the materials but mainly the topologies, routes, and safety design of each installation, would ensure the uniformity of all offers (regardless of the manufacturer), and directly yield financial benefits.

To better understand the level of difficulty, we analyzed all categories and subcategories referenced in the Tender Document and reclassified them to clarify the subject. As you can see, all requirements fall into sixteen (16) different general categories:

1. SECURITY SYSTEMS

a. [Tender Document – Chapter #1] – CCTV Video Surveillance Systems

Paragraphs: 1.1, 1.2, 1.3, 1.4, 1.5, 1.8, 1.10, 1.11, 1.12, 1.13, 1.14, 1.15, 1.16, 1.17, 1.18, 1.19, 1.20

b. [Tender Document – Chapter #2] – Security Systems (Intrusion Detection)

Paragraphs: 1.9, 2.1, 2.2, 2.3, 2.4, 2.6, 2.7, 2.8, 2.9, 2.10, 2.11, 2.12

c. [Tender Document – Chapter #3] – Access Control Systems

Paragraphs: 3.1.1, 3.2, 3.3, 3.4, 3.5, 3.7, 3.8, 3.9, 3.11, 3.12

d. [Tender Document – Chapter #4] – Conventional Fire Detection Systems

Paragraphs: 4.1, 4.2, 4.3, 4.4

e. [Tender Document – Chapter #5] – Addressable Fire Detection Systems

Paragraphs: 5.1, 5.2, 5.3, 5.4, 5.5

f. [Tender Document – Chapter #9] – Ancillary Installations

1. Chapter 9.1 – Unified Field Intercom Communication Unit
2. Chapter 9.2 – Monitor / Intercom Console
3. Chapter 9.3 – Warning / Alert Signage
4. Chapter 9.8 – Connection Cabinet
5. Chapter 9.9 – External Pillar
6. Chapter 9.10 – IT/Networking Equipment Cabinet (Field)
7. Chapter 9.12 – UPS Units (Field)
8. Chapter 9.13 – Racks for Hosting Equipment
9. Chapter 9.15 – C&C and Data Room Racks
10. Chapter 9.19 – IT Management of Facility Systems

g. [Tender Document – Chapter #12] – Installation Implementation Services

Paragraphs: 12.1, 12.3.6, 12.3.7, 12.3.8, 12.3.9, 12.4.1

h. [Tender Document – Chapter #13] – Technical Support Operation Services

Paragraphs: 13.1.1, 13.1.2, 13.2.1, 13.2.2, 13.2.3, 13.2.4, 13.4

2. NETWORKING

a. [Tender Document – Chapter #8] – Communication Network

Paragraphs: 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8, 8.9

3. OPERATIONAL CENTERS

a. [Tender Document – Chapter #10] – Operational Centers (C&CC)

Paragraphs: 10.1, 10.2, 10.3, 10.4, 10.5, 10.8, 10.9, 10.10, 10.11, 10.12, 10.13, 10.14, 10.15, 10.16, 10.17, 10.18, 10.19, 10.20, 10.21, 10.24, 10.25, 10.24.5

4. SUPPRESSION SYSTEMS

a. [Tender Document – Chapter #9 / Paragraph 9.29] – Building Suppression Systems

b. [Tender Document – Chapter #9 / Paragraph 9.30] – Portable Dry Powder Fire Extinguishers

c. [Tender Document – Chapter #9 / Paragraph 9.31] – Portable CO2 Fire Extinguishers

d. [Tender Document – Chapter #10 / Paragraph 10.22] – Suppression Systems for C&CC and Data Room

5. ELECTRICAL WORKS & MATERIALS

a. [Tender Document – Chap. #9 / Paragraph 9.4] – Wall-Mounted Lighting Fixtures

b. [Tender Document – Chap. #9 / Paragraph 9.5] – Floodlight-Type Lighting Fixtures

c. [Tender Document – Chap. #9 / Paragraph 9.6] – Automated Lighting Control Systems

d. [Tender Document – Chap. #9 / Paragraph 9.17] – Facility Distribution Substations

e. [Tender Document – Chap. #9 / Paragraph 9.18] – Power Supply Services

f. [Tender Document – Chap. #10 / Paragraph 10.7] – C&CC Distribution Substations

g. [Tender Document – Chap. #10 / Paragraph 10.20] – C&CC Cabling

h. [Tender Document – Chap. #10 / Paragraph 10.25.1] – Electrical Works (C&CC)

i. [Tender Document – Chap. #11] – Facility System Cabling & Infrastructure

Paragraphs 11.1, 11.2, 11.3

j. [Tender Document – Chap. #12 / Paragraph 12.3.1] – Electrical/Mechanical Works MEN-KEK

k. [Tender Document – Chap. #12 / Paragraph 12.3.2] – Electrical/Mechanical Works Offices-Counters

l. [Tender Document – Chap. #12 / Paragraph 12.3.3] – Electrical/Mechanical Works Other Facilities

6. TELECOMMUNICATION SUBSCRIPTIONS

a. [Tender Document – Chap. #2 / Paragraph 2.5.1] – Global SIM Subscriptions

b. [Tender Document – Chap. #8 / Paragraph 8.10] – Mobile Telephony Subscriptions

c. [Tender Document – Chap. #8 / Paragraph 8.11] – Telecommunication Subscriptions for Large Facilities

d. [Tender Document – Chap. #8 / Paragraph 8.12] – C&CC Telecommunication Subscriptions

7. CYBERSECURITY

a. [Tender Document – Chap. #12 / Paragraph 12.2.1] – Cybersecurity Study Services

b. [Tender Document – Chap. #13 / Paragraphs 13.3.1, 13.3.2, 13.3.3] – Cybersecurity Services (SOC)

8. AERIAL SYSTEMS

a. [Tender Document – Chap. #7] – Drone Systems

b. [Tender Document – Chap. #12 / Paragraph 12.4.2] – Drone Operator Training Services

9. SECURITY PERSONNEL & VEHICLES

a. [Tender Document – Chap. #14 / Paragraph 14.1] – Static Guarding & Foot Patrols

b. [Tender Document – Chap. #14 / Paragraph 14.2] – Security Personnel

c. [Tender Document – Chap. #14 / Paragraph 14.3] – Patrols with Vehicle

d. [Tender Document – Chap. #14 / Paragraph 14.4] – Firefighting Vehicles

e. [Tender Document – Chap. #14 / Paragraph 14.6] – First Aid Kit

10. MANAGEMENT & EQUIPMENT FOR SECURITY PERSONNEL

a. [Tender Document – Chap. #1 / Paragraph 1.6] – Portable Scanner

b. [Tender Document – Chap. #1 / Paragraph 1.7] – Portable Data Storage Station and Transport Stand

c. [Tender Document – Chap. #9 / Paragraph 9.25.1] – Guard Patrol Management System

d. [Tender Document – Chap. #9 / Paragraph 9.25.1] – Patrol Checkpoint Monitoring System

e. [Tender Document – Chap. #9 / Paragraph 9.25.2] – QR Tag Printer

f. [Tender Document – Chap. #9 / Paragraph 9.25.3] – Terminal Device QR Code Integration

g. [Tender Document – Chap. #9 / Paragraph 9.26] – AR Glasses

11. PROTECTIVE EQUIPMENT

a. [Tender Document – Chap. #9 / Paragraph 9.22] – Explosion Suppression Blanket

b. [Tender Document – Chap. #9 / Paragraph 9.28] – Anti-Vandalism Security Membrane

12. X-RAY & METAL DETECTION DEVICES

a. [Tender Document – Chap. #9 / Paragraph 9.20] – X-Ray Screening Device for Rolling Luggage

b. [Tender Document – Chap. #9 / Paragraph 9.21] – X-Ray Screening Device for Small Parcels

c. [Tender Document – Chap. #9 / Paragraph 9.23] – Magnetic Gate for Metal Detection

d. [Tender Document – Chap. #9 / Paragraph 9.24] – Handheld Metal Detectors

13. OTHER SYSTEMS

a. [Tender Document – Chap. #6] – Key Management Systems

Paragraphs: 6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7

b. [Tender Document – Chap. #9 / Paragraph 9.18] – Electronic Lockers

14. AIR CONDITIONING UNITS

a. [Tender Document – Chap. #3 / Paragraph 3.16] – Data Room Air Conditioning Systems

15. METALLIC CONSTRUCTIONS & MATERIALS

a. [Tender Document – Chap. #3 / Paragraph 3.6] – Door Replacement Mechanisms

b. [Tender Document – Chap. #3 / Paragraph 3.10] – Electromechanical Traffic Barrier

c. [Tender Document – Chap. #9 / Paragraph 9.7] – Lifting Mast

d. [Tender Document – Chap. #9 / Paragraph 9.14] – Single-Leaf Metal Door

e. [Tender Document – Chap. #9 / Paragraph 9.15] – Double-Leaf Metal Door

f. [Tender Document – Chap. #9 / Paragraph 9.27] – Motorized Garage Door

g. [Tender Document – Chap. #9 / Paragraph 9.32] – Fence Installation at Points of Interest

16. OTHER WORKS

a. [Tender Document – Chap. #12 / Paragraph 12.3.4] – Disinfection Services

It is clearly evident that the implementation of this specific project is not feasible without causing serious damage to your company.

From our side, we are at your disposal to provide any additional information or clarification.

Comments by Economic Operator 4

Good morning,

With reference to the Technical Specifications (Tender Documents) of the project: "Integrated Digital System for the Management of Electronic & Physical Security,

including the Provision of Security and Fire Safety Services at the Facilities of EYDAP S.A." by EYDAP S.A. (Athens Water Supply and Sewerage Company), which our company received in order to submit its proposals within the framework of the Public Preliminary Market Consultation, in accordance with Article 278 of Law 4412/2016, as amended and in force, and the Procurement and General Services Regulation of EYDAP S.A., regarding the Integrated Digital System for the Management of Electronic and Physical Security, with the provision of Security and Fire Protection Services at EYDAP S.A. facilities, our company would like to propose the following:

Regarding the Drone (UAS) Service:

Reference to this service is limited to pages 30 and 57, specifically under section 12.4.2 "UAS (Drone) Operator Training Services" of the Technical Specifications document.

Regarding the above-mentioned Drone (UAS) service, our company proposes the following:

On page 57, paragraph 12.4.2, the reference to the "UAS Instructor" should be removed, as according to EASA Regulation 2019/947, the role of Instructor no longer exists.

Additionally, in the same paragraph, the phrase: “maintenance instructions for the equipment as well as training material in electronic format, beyond the UAS operating manuals, will be provided” should also be removed. This is because each manufacturer defines the maintenance program and instructions for the UAS, which are either included in the technical manual or in the UAS software, and each user is required to follow them. These instructions cannot be provided as additional guidance by the contractor but only referred to during the theoretical training of the Contracting Authority’s personnel.

As for the training material in electronic format, this can only be provided if it is made available by the UAS manufacturer, in order for the UAS operators to have access to any relevant updates.

Regarding the Fire Safety Coordinator and Deputy Coordinator, as referenced in section **14.2.2 of the Technical Specifications** (page 82):

Page 82 of the Technical Specifications states that: "The service provider shall designate one individual to be referred to as the Fire Safety Fleet Coordinator (a certified engineer or technician with at least 20 years of experience)."

The requirement for a minimum of 20 years of experience for the Fire Safety Coordinator, as currently defined, unnecessarily restricts free competition and conflicts with the principles of equal treatment and transparency as protected by applicable EU law.

The intended purpose of this requirement — ensuring proper fire protection of EYDAP's sensitive facilities — can be achieved just as effectively through less restrictive means that promote competition.

Therefore, while our company agrees that a minimum experience criterion is reasonable for the roles of Fire Safety Coordinator and Deputy Coordinator due to the critical importance of fire protection, we propose the following adjustments:

- Reduce the minimum required experience for the Fire Safety Coordinator from 20 years to 10 years in the relevant field (Engineer or Technician).
- Similarly, reduce the minimum experience for the Deputy Coordinator from 10 years to 3 years in the same relevant field.

This proposed modification maintains the necessary level of expertise and competency, while promoting greater access to competition.

Regarding the Fire Safety Vehicles

(Section 14.4 of the Technical Specifications)

In reference to the fire safety vehicles listed under section 14.4 of the Technical Specifications, and specifically the table on page 87, we have identified the following inconsistency: While section (c) of clause 14.4.2 concerning the Equipment of Firefighting Station Vehicles (page 90 of the Technical Specifications) states:

"c. The water tank (or other extinguishing agent) of each firefighting station must have a capacity of at least 600 liters with an outlet for fire extinguishing."

In the table on page 87 referring to the firefighting vehicles, there are vehicles listed with tank capacities of 700 liters as well as others with capacities of 2000–3000 liters.
Our company proposes that the specified tank capacity of the firefighting vehicles be limited to a maximum of 600 liters, for the following reasons:
Typically, pickup-type vehicles have a payload capacity of around 1,000 kg. Considering the following:

- The weight of the water alone is 600 kg
- The full weight of the superstructure is approximately 180 kg
- The weight of the two passengers, including their equipment, is around 90 kg each

The total of the above approaches the maximum allowable payload of such vehicles.
As a result, tanks exceeding 600 liters pose a potential safety risk for passengers, as they increase the likelihood of vehicle rollovers, and consequently, accidents. These not only endanger the physical safety of the occupants but also jeopardize the effective and timely response to fire incidents.
In contrast, vehicles with smaller tank capacities (i.e., up to 600 liters) can be fitted onto smaller, more compact, and therefore more agile vehicles, which can respond faster and more effectively to fire incidents than larger vehicles.
In any case, the role of these vehicles is intended to be supportive, primarily focused on the initial outbreak of fires. It is understood that they are not expected to handle large-scale fires, which would fall under the responsibility of the Fire Department.
Thank you very much, and we remain at your disposal for any clarification or comment.

Comments by Economic Operator 5

1. CCTV Video Surveillance System

1.1 Perimeter Surveillance Camera

It is proposed that the perimeter surveillance camera be equipped with a multi-lens system.
Its power supply should support 12V DC, PoE, with a maximum consumption of 15W.
The image resolution is recommended to be at least 4MP, ensuring high quality, improved sharpness, and clarity.

Additionally, AI technology should be one of its core features.
With the use of AI, the system can implement line crossing rules, triggering alerts when there is an intrusion into a designated area by specific targets (e.g., human or vehicle).
Finally, where necessary, the camera should offer anti-corrosion protection.

1.2 Entry-Exit Control Camera

It is proposed that this camera should have a lens of at least 2.8 mm.
Its power supply should support 12V DC, PoE, with a maximum consumption of 12W.
The image resolution is recommended to be at least 4MP, ensuring high quality, improved sharpness, and clarity.
Finally, it is recommended that the camera is capable of providing color images even in low-light or night conditions.

1.3 Outdoor Installation Camera

For cameras to be installed in large-scale facilities, such as dams, it is proposed that they be equipped with specialized functionality capable of providing information on water levels, as well as underwater cameras that perform a broader monitoring of water quality, in accordance with the relevant authority's guidelines.
The cameras offered must be constructed with anti-corrosion materials to ensure durability under harsh outdoor conditions, and they should support a resolution of 4MP.

1.9 Security Radar

It is proposed that the security radar, in cases where it is installed at a large-scale facility (e.g., a dam), should have a range greater than 500 meters in order to adequately cover such extensive areas without issue.
Its installation should be accompanied by a PTZ-type security camera, and the system should be capable of simultaneously tracking up to 32 different targets.
It is also proposed that the radar should support up to 16 different detection zones, ensuring comprehensive surveillance of open areas.

1.10 PTZ Outdoor Camera

For PTZ cameras to be installed at large-scale facilities (e.g., a dam), it is proposed to install PTZ cameras are equipped with both optical and thermal lenses to ensure enhanced monitoring capabilities over the area. These cameras should perform patrols based on multiple active scenarios, monitoring for unauthorized entries, perimeter breaches, and temperature readings above the predefined limits.

Furthermore, due to their critical role, the cameras must be able to perform scheduled patrols within their designated responsibility zones. They should also be self-cleaning, ensuring uninterrupted functionality at all times. Finally, the sensor unit must come with a minimum warranty of 8 years.

1.11 Acoustic Deterrent Loudspeaker

It is proposed that the loudspeaker and by extension the entire public address system should be IP-based rather than analog. This will allow for easier scalability and enable all available functions to operate via the same network cable that will be installed for the operation of the surveillance cameras.

7. Unmanned Aerial Vehicles (Drones)

It is proposed that the drones be equipped with special ground docking stations from which they take off and to which they return, so that they can be recharged without operator intervention.

Additionally, they should be capable of autonomously conducting predefined patrols in designated responsibility areas and allow for remote flight management by a licensed operator from the control center (STS01 – 02). They should also be capable of saving video footage to the cloud for enhanced data security.

The drone should be automatically triggered to take flight in case of an alarm signal from any existing or non-existing ground security system, fire alarm, or notification from a surveillance camera.

It must be capable of flying in winds up to 8 Beaufort and be fully waterproof.

8. Communication Network

8.1. Field Network Equipment & 8.2. Peripheral Network Equipment

It is proposed that, for the needs of the peripheral points (ring topology), IoT BOX security enclosures with built-in alarm systems be installed.

These should include a PoE switch with optical ports and a battery capable of providing at least 12 hours of uninterrupted power at 60 watts.

Additionally, it is proposed that there be 12V output for the connection of a security floodlight in case of a power outage.

Finally, there should be the option to add a solar panel to extend the uninterrupted operation time.

8.3 Central Network Equipment

It is proposed that, for the needs of the central infrastructure, the switches be fully Layer 3 capable, with inter-VLAN routing functionality. Additionally, it is recommended that the switches support stacking to ensure the uninterrupted operation of the network.

9. Installation Accessories

9.20 X-Ray Conveyor Scanner Device

It is recommended that the tunnel dimensions be slightly larger than 60x40 (e.g., 65x45) so that it can comfortably accommodate backpacks without issues. Additionally, the system should include incoming baggage counters for historical tracking, as well as a fully diagnostic tool for self-checking its functions.

It is also proposed that it features two monitors of at least 23 inches to allow for better control by the system operator.

Furthermore, it is recommended that the system be from the same manufacturer as the proposed cameras, allowing for centralized management through the Security Operations Center (SOC).

Finally, it is suggested that the offered machine supports login via biometric identification, such as facial recognition, fingerprint scanning, and password entry to ensure enhanced

security, preventing unauthorized access or tampering by anyone other than the authorized operator.

10. Operations Centers

For the overall setup of the operations centers, it is recommended that the company undertaking this critical part of the project should have independently constructed and put into full operation two proprietary alarm and image signal receiving centers that have been functioning simultaneously, bidirectionally, as well as independently (if required) for at least three years. This requirement ensures that the company possesses the necessary experience and expertise to guarantee their smooth operation.

10.13 Alarm System Software, 10.15 Access Control System Software, etc.

Regarding the software of the individual subsystems, it is recommended that a unified software platform be used for the alarm system, access control, CCTV, X-Ray, and public address systems.

This approach offers:

- Maximum security,
- Full integration of all systems,
- Simplified operation for the user, and
- Reduced response time in the event of incidents.

14. Security Services

For the physical guarding component, it is recommended that an on-site inspection be conducted at each facility individually to ensure that all areas are adequately covered and that no security gaps exist.