

Questions and Answers (Q&A)

*in relation to the Request for Expression of Interest (EOI)
to identify and evaluate Physical Security Platform*

No.	Question from the Vendor	Answer from the IAEA Requesting Office/ Office of Procurement Services
Q&A no. 1; release date: 2 March 2020		
1.	We have developed platforms that do what you need, but they are proprietary and not open architecture. I kindly ask you to let me know if you would like to know more details about what we can offer.	The IAEA is interested in non-proprietary with an open architecture platform
2.	WHAT IS YOUR BUDGET	The IAEA does not disclose its budget for this project
3.	PUBLIC OFFER OF DIRECT CONTRACT	This objective of this EOI is to identify and short-list Vendors and their respectful Physical Security Platforms (Project Phase I); the Request for Proposal (tender) will be sent only to short-listed Vendors.
4.	open non-proprietary system specify? you can't ask directly	Please see IAEA answer to the Question no. 1
5.	all run under corporate LAN - separate LAN with dedicated server - offices not connected	This question is not relevant to this phase of the project. The physical security network is on its own isolated network
6.	replacement of identification systems with restricted access? see magnetic card systems or facial recognition. iris etc.	We are interested in an card based system – not a biometric system
7.	Should access be blocked? I think not for safety	The system must abide by Austrian safety regulations and building codes

8.	Must accesses be recorded and how long is memory kept?	Access must be recorded and stored for a 12-month period
9.	video surveillance systems with anthropometry recognition	No, facial recognition is not a requirement
10.	CURRENT USED SYSTEM, WHAT CRITICALITY?	The current system is a proprietary Legic based access control system
Q&A no. 2; release date: 6 March 2020		
11.	<p>Re: “ Question 10 quality “</p> <p>The EUROPEAN standard EN 50131 is the European standard series for intruder alarms and hold-up systems. Fully understand that any intrusion alarm system replacement required in this upgrade should meet the EN 50131 standard.</p> <p>However Access Control and CCTV platforms are not mentioned in or tested to EN 50131 intruder standard - but are part of EN50133 guidelines.</p> <p>Therefore my question is who determines what grade the Access Control and CCTV equipment will meet?</p> <p>is it the IAEA or an independent body where we need to submit our equipment?</p>	<p>Ref. EOI-356334-YG – Questionnaire/Quality_Req/Criterion 10</p> <p>To clarify, the scope for CCTV within this project is to integrate the IAEA existing solution with your product. Regarding the grading of the Access Control component, the IAEA technical experts will take a holistic view of the entire integrated platform in order to evaluate the security of the solution.</p>
Q&A no. 3; release date: 11 March 2020		
12.	Migration of a single door – Is it a new installation or currently there is a system that we need to interface with?	Phase 1 is the collection of information for the available products in the market. Phase 2 will be a pilot. During the pilot you will not interface with any of our existing access control or intrusion systems. You will however interface with the existing electromechanical locks, sirens and strobes. You may interface with the existing card readers,

		unless you propose a newer reader technology and can show the benefits or replacing them.
13.	Require compatibility with the following controllers: HID VertX controllers, Mercury Security controllers, Axis A1001/A1601 Network Door Controller; Does that mean that these controllers are already installed, and that they are using Access Control management System like Genetec “Synergis Security Center” ? or any similar? If so, does the migration plan (and PoC) includes integration to (and migration from) an existing Access Control Management System?	We do not currently own any of these “open architecture” controllers. In the future we would like to move in this direction for reasons of flexibility. For the second phase of this project we would like to pilot one of the proposed systems from phase 1 (EOI phase). Whether that will be on new doors or doors with an existing alarm system will be decided later. This is not something you need to worry about at this point. Please just tell us whether your proposed PSP supports any of the items in the matrix and whether there are any limitations (reflashing of code, limited functionality etc).
14.	Of all the requirements mentioned in the document what are the parameters that are going to be tested in the PoC?	If your proposal is selected as a potential candidate for the POC, you will have the chance to tour our facility as part of phase 2. Once you see what we have we can discuss how you might configure your proposed system to use existing components or not.
Q&A no.4; release date: 30 March 2020		
15.	Could you provide us with the technical specifications of the access control sensors and cameras, including the connectivity interfaces?	<p>The following devices meeting this question are installed and in use at this time:</p> <p>Alarm/Access control “sensors”:</p> <ul style="list-style-type: none"> • Honeywell Viewguard DUAL AM BUS-2 for rooms requiring alarm/intrusion capabilities. These devices are directly connected via BUS-2 to the Honeywell intrusion detection system. Note: PIN-pad access control readers are used to arm/disarm these detectors via external Input/Output configurations on both, the access control as well as the intrusion alarm system.

		<ul style="list-style-type: none"> • Reed-contacts and recessed reed contacts: Honeywell 030810.16, 030260.16, 030261.16, 030270, 030271, 030270.06, 030271.06 Class C. Directly wired to (Bus-2) enabled alarm controllers. • Standard bolt-switch contacts, sabotage and feedback outputs of all electronic locks as per compatibility list (DIN, Abloy, BKS) directly wired to access control modules or their IO expansion boards. • Access control readers as per compatibility Matrix wired directly to access control modules using WIEGAND interface.
16.	<p>In relation to the pilot plant, you would require:</p> <p>a) Hardware controllers;</p> <p>b) Software\Licenses; and</p> <p>c) Labour effort and timeline</p> <p>and to consider “IAEA’s existing requirements, wiring, and peripherals.”.</p> <p>What do you consider necessarily needed and included as “Labour effort” by the vendor of the pilot plant?</p>	<p>Phase two of this effort is to select a vendor to perform a proof of concept pilot. This pilot will require everything needed to implement the proposed platform for a subset of doors in a selected area of the facility. The amount of labour required will be whatever is needed to implement the pilot. The labor can be provided by the vendor or a local partner / reseller. Preferably we would have the opportunity to interact with whomever would be supporting the installation in the event is were adopted. We expect to pay for the pilot and are not asking vendors to provide this service free of charge. Again – this is the second phase, for phase 1 we want to gather information of how well your platform will fit our environment.</p>
17.	<p>If we don’t want to participate with selected local and we imply that the physical installation work can be demanded to IAEA/UNO buildings networking equipment installers and to electricians who connected the existing electrified door-locks. Is this compatible with the participation to your EOI/RFP?</p>	<p>If you are proposing a platform you need, at the very least to have one of your authorized resellers participate in the pilot. If you feel that the system is simple enough that we can support it in-house, your reseller would still need to participate in the pilot in order to demonstrate the simplicity of the integration and provide some transfer of knowledge.</p>
18.	<p>About the personnel qualification, labor and installation norms. You ask for compliance to:</p> <p>IEC 60634 -> LOW VOLTAGE</p> <p>IEC 60297 -> 19" Racks</p>	<p>Please include this information in your submission for phase-1. If your proposed platform does not require any high voltage requirements this is not an issue. I see no reason why this is not compatible for consideration for the phase-2 pilot.</p>

	<p>EN 50173-174-> CAT5 and superior structured cabling.</p> <p>And that “Any Vendor invited to participate in a pilot must either be qualified or subcontract with a local qualified electrician to perform low and high voltage cabling and electric installations associated with the implementation of the physical security platform.”</p> <p>The Low Voltage definition is from 50...70V to 600V..1KV (depending on local norms), and High Voltage from 0.6-1KV to 33KV-36KV, so it is not clear why High Voltage would be a concern.</p> <p>Our PSP proposal could be implemented using only ELV (Extremely low voltage <60Vdc) power devices, namely the 48Vdc of PoE (Power over Ethernet) for controllers, and 12Vdc for the readers, generated by our PoE controllers.</p> <p>We would not sell nor install PoE Ethernet Switches which would be the sole 19” rack devices. Our controllers must be mounted on DIN rails, and enclosed in wall-mount panels.</p> <p>Is this compatible with the participation to your EOI/RFP?</p>	
<p>19.</p>	<p>For the pilot phase, you ask to use the existing peripherals, and for sure Wiegand or OSDP RFID readers are in our basket. But BUS-2 devices can't be used out of Honeywell controllers, and Lumiprox readers by G4S/T, repeated in three variations on the readers section, are completely unknown by the market and doesn't appear to have public technical documentation.</p> <p>What was your idea about the use of IAEA existing intrusion detection and alarming peripherals, and Lumiprox readers?</p>	<p>We were interested in whether the proposed platform might support any existing peripherals. If a good case can be made to replace existing peripherals please explain how that might benefit us. We need at least a good reason why reinvestment in peripherals should be considered.</p>