



Info-communications Media Development Authority (IMDA)

Requirements for Integrated Security Management (ISM) Solutions for Security Sector

Date Issued: 4th Aug 2023

Version: 1.0

1. IMPORTANT NOTE

- 1.1 This document must be read in conjunction with the information on [Security Industry Digital Plan](#) and [Advanced Digital Solutions \(ADS\)](#).

2. CALL FOR PROPOSALS

- 2.1 Info-communications Media Development Authority (IMDA) and Ministry of Home Affairs (MHA) are calling for proposals to aid small and medium-sized security agencies in delivering value-added services beyond basic guarding to security service buyers (i.e., building owners, managing agents, etc.) through using integrated technologies.
- 2.2 The intent is to raise the capabilities of small and medium sized security agencies to integrate operations to deliver higher quality services via centralised technological platforms. In doing so, security service buyers can benefit from better services and potential cost savings whilst security officers are upskilled to take on more meaningful job roles.

3. BACKGROUND

- 3.1 The Security Industry Transformation Map (ITM), led by MHA with support from tripartite partners including IMDA, was launched in 2018 to uplift the private security industry. The ITM has since helped the industry move progressively from a manpower-intensive model to one that integrates skilled manpower and technology to deliver higher quality security services.
- 3.2 In 2022, the Security ITM 2025 was launched to build on this momentum by pressing on with refreshed initiatives as well as preparing the industry for the new model of delivering security, cleaning, and facilities management services as part of integrated facilities management (integrated FM).
- 3.3 To support the ITM 2025, MHA and IMDA are jointly updating the Security Industry Digital Plan (IDP), so that it remains relevant to the needs of security agencies and supports the growth of their digital capabilities. This includes the Call-for-Proposal (CFP) outlined above in para 2.1.
- 3.4 Further, the shift towards integrated FM implies that security services will be integrated and coordinated with other facility management functions, allowing for a more comprehensive and efficient approach to security provision.

- 3.5 The Security ITM and IDP have guided the security industry to adopt solutions featured in the digital roadmap. For example, some medium-sized security agencies have since implemented the Security Collaboration Platform (SCP) to build their integrated security command centres, which have enabled them to guard buildings with minimal or no officers on-site.
- 3.6 Consultations with the industry revealed there are opportunities for small and medium-sized security agencies to provide the additional services¹, on top of security requirements, to meet service buyers' needs. The additional services can include:
- a. Monitoring cleanliness of toilets, toilet expendables, alerting cleaners to clean the toilets, replenish the expendables (toilet paper, hand soap), or alerting in the event of a slip, trip or fall incident;
 - b. Monitoring fire and smoke emergency incidents in the building or the fire-safety equipment (e.g., exit signs and fire extinguishers) to ensure fire incident can be detected as early as possible or the fire-safety equipment remain functional, and alerting maintenance staff for appropriate follow up actions as required;
 - c. Monitoring the rate of energy and water consumption to ensure that they are within acceptable thresholds and alerting responsible parties to identify measures to ensure prudent usage; and
 - d. Monitoring air quality within buildings to help identify various pollutants hotspots and contaminants in the air to make sure that the building is safe for occupants to breathe and comfortable spaces for occupants.
- 3.7 This CFP invites consortiums consisting of technology solution providers, security agencies and security service buyers to build and pilot ISM² solutions that enable higher quality and cost-effective integrated services to security service buyers.
- 3.8 While this CFP seeks to deliver ISM solutions that are integrated with fixed number of defined 3rd party monitoring solutions, it is envisioned that the ISM would eventually develop into an interoperable platform that allows integration with any 3rd party monitoring solutions through, but not limited to, industry-wide standardisation. This will provide security service buyers with higher flexibility and control whenever there are changes in contract service providers.

¹ This list of services is non-exhaustive.

² IMDA and MHA reserves the right to make changes to the tentative Integrated Security Management (ISM) solution category name.

4. FUNCTIONAL REQUIREMENTS

This section specifies the functional requirements of ISM.

4.1 The core of ISM comprises 2 key components:

- a. **Management Dashboard**, to provide a holistic view of aggregated data, situational awareness, and high-level strategic insights. This allows building owners or security supervisors to make informed decisions based on executive summaries of building performance and key trends; and
- b. **Operational Dashboard**, to provide real-time visibility into processes and metrics such as fire safety, security incidents, and more. This enables security officers to monitor operations, track performance, and respond to critical events effectively.

4.2 **[Mandatory]** ISM must include management dashboard that provide high level summary insight for holistic view of situational awareness, aggregated data, executive summary of building performance. For example: Top 10 security incidents, fire equipment breakdown trends, monthly toilet cleaning schedule optimization, or month to date energy consumption. Management dashboard will enable building owner or management of security company (security supervisor) obtain high-level strategic insights, and overall building performance to make informed decisions.

4.3 **[Mandatory]** ISM must include operational dashboard that provides real-time visibility into operational processes, real-time insights of operational metrics, performance indicators of real time information on operational activities, live feeds, alerts, or notifications. For example: Real time data reading of fire safety equipment, exit light status, toilet smell / pollutant index, soap dispenser status, security incident and unauthorized visitor attempt, loitering or unattended bag monitoring, etc. Operational dashboards will enable security officers to monitor operational processes, track performance, keep them informed about critical events or changes during day-to-day operational management.

4.4 **[Mandatory]** ISM must include real time monitoring, alert and notification with mitigation/ SOP action that keep security officer informed during any events, incident, issues, or emergency. For example: Real time alert/ alarm during fire incident that allow security officers to activate evacuation plan, water leakage that allow security officers to send notification to cleaner/ plumber, people fall in toilet, unattended bags, or suspicious objects, or unhealthy air quality.

4.5 **[Mandatory]** ISM must include predefined & dynamic workflow management, orchestration that streamlines various processes. For example: Automatically notifying security officers, locking down specific areas, dispatching emergency services when a

fire alarm is triggered, and alert security officers if there are water pipe leakage followed by subsequent notification to cleaner/ plumber.

- 4.6 **[Mandatory]** ISM must include reporting feature that generate report of analysed data in a user-friendly and actionable manner (e.g., key metrics reports/ charts with clear overview metrics related with fire equipment fault, toilet cleanliness index, security incident, or energy consumption, maintenance response time, building energy performance, etc.).
- 4.7 **[Mandatory]** ISM must integrate with a Security Collaboration Platform (e.g., with the capabilities of Incident Management, Online Surveillance & Analytics, and Risk Thread Detection & Prediction) as part of this project, which can be an existing/deployed platform (Annex A – model A) or a 3rd party Security Collaboration Platform (Annex A – model B).
- 4.8 **[Mandatory]** ISM must integrate with Fire Safety and Emergency Monitoring Solution to monitor, detect, mitigate, and provide rapid responses such as evacuation and real-time incidents reporting during fire and smoke emergency incidents. This integration will enable security officers to monitor, control, manage emergency incident or maintain fire safety equipment (such as fire extinguishers, exit lights) in serviceable condition.
- 4.9 **[Mandatory]** ISM must integrate with Toilet Cleaning Management Solution to monitor the state of toilet, usage, and condition of toilet in real-time such as footfall or human traffic, air quality, gas monitoring, water pressure/ flow rate, floor wetness/ water pipe leakage, bin level, occupancy, motion, paper towel dispenser, and soap dispenser availability. This integration will enable security officers to monitor cleanliness of toilet situation, dispenser availability of toilet assets as well as the safety of toilet usage.
- 4.10 **[Optional]** ISM integrates with Energy Consumption Monitoring Solution to monitor, analyse, and manage power, electrical, water and energy consumption to optimize resource usage, promote sustainable practices, energy efficiency, sustainability reporting, reduce environmental impact of a building and report on the sustainable practices. This integration will enable security officers to provide constructive feedback to service buyer or building owner on energy consumption of building, as well as identified area that consume most energy and any equipment that that need ad-hoc maintenances due to current overload.
- 4.11 **[Optional]** ISM integrates with Indoor Air Quality Monitoring Solution to monitor and measure the air quality within building environment to help identify various pollutants hotspots and contaminants in the air and inform decision-making on how to improve air quality to make sure that the building is safe for occupants to breathe. These sensors can detect a variety of pollutants and factors that may affect air quality (e.g., Temperature, Humidity, VOC, CO₂, CO, NH₃, PM, etc). This integration will enable security officers make sure that the building is safe for occupants to breathe while

improve occupant comfort, productivity and create healthier as well as more comfortable spaces for occupants.

4.12 **[Mandatory]** ISM must enable ease of activating or de-activating 3rd party monitoring solutions that have been integrated within ISM, through system configuration or administration module.

4.13 **[Mandatory]** To demonstrate the compatibility of the solution with its target service buyer/building type, ISM is expected to be deployable in at least 3 buildings of similar typology (e.g., 3 industrial buildings of similar FM service requirements) within the same proposal, as part of onboarding Participating Companies onto the project under the ADS grant.

4.14 Please refer to:

- [Annex A](#) for the 2 suggested integration models of ISM; and
- Section 4.2 “Good Practices to Facilitate Data Management” of the [Guide to Smart FM](#) for the open communication protocol/ data schema standards.

5 PROPOSAL SUBMISSION

5.1 Please use this [form](#) to indicate your interest to participate in this CFP.

5.1.1 IMDA shall conduct an initial assessment to pre-qualify the participants; and

5.1.2 CFP briefing(s) will be scheduled with the pre-qualified participants, who are required to attend a briefing session before submitting proposal(s) to IMDA.

5.2 To be considered for ADS grant support, you are required to submit complete proposal(s) to suganda_ekaputra_sidharta@imda.gov.sg; tan_choon_huat@imda.gov.sg; chan_yew_kee@imda.gov.sg by **8th September 2023**. Respondents with complete proposal(s) will receive an acknowledgement.

IMDA reserves the right to reject incomplete or late submission(s).

5.3 Complete proposals received by 8th September 2023 will be evaluated by IMDA for ADS grant support eligibility. IMDA and MHA reserve the right to make the final decision on proposal approval.

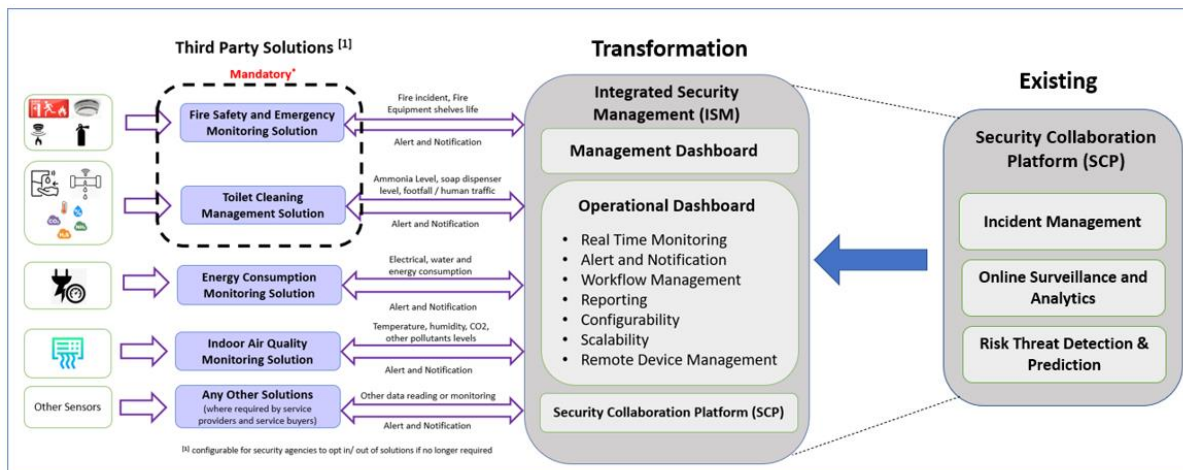
If your proposal is approved, you will be notified by IMDA within 3 months from submission date.

[End of Document]

Annex A

The diagrams below illustrate the suggested integration models of the Integrated Security Management (ISM).

Model A: SCP solution with enhancement and integration with mandatory 3rd party solutions



Model B: "Integration-as-a-Service" platform that integrates with mandatory 3rd party solutions

