Info-communications Media Development Authority (IMDA)

Requirements for

Risk/Threat Prediction and Detection (RTPD)

for Security Sector

Date Issued: 19th July 2024

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 inviting industry partners either individually or as part of a consortium (led by a single industry partner), to submit proposals for a cost-effective "Risk/Threat Prediction and Detection" solution. The solution shall enhance the situation awareness of small and medium-sized security agencies through continuous monitoring and early threat detection.

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 catalysing greater adoption of advanced and inter-operable technology.

3.3 To support the ITM 2025, MHA and IMDA have jointly updated the Security Industry Digital Plan (IDP) in Nov 2023, so that it remains relevant to the needs of security agencies and supports the growth of their digital capabilities.

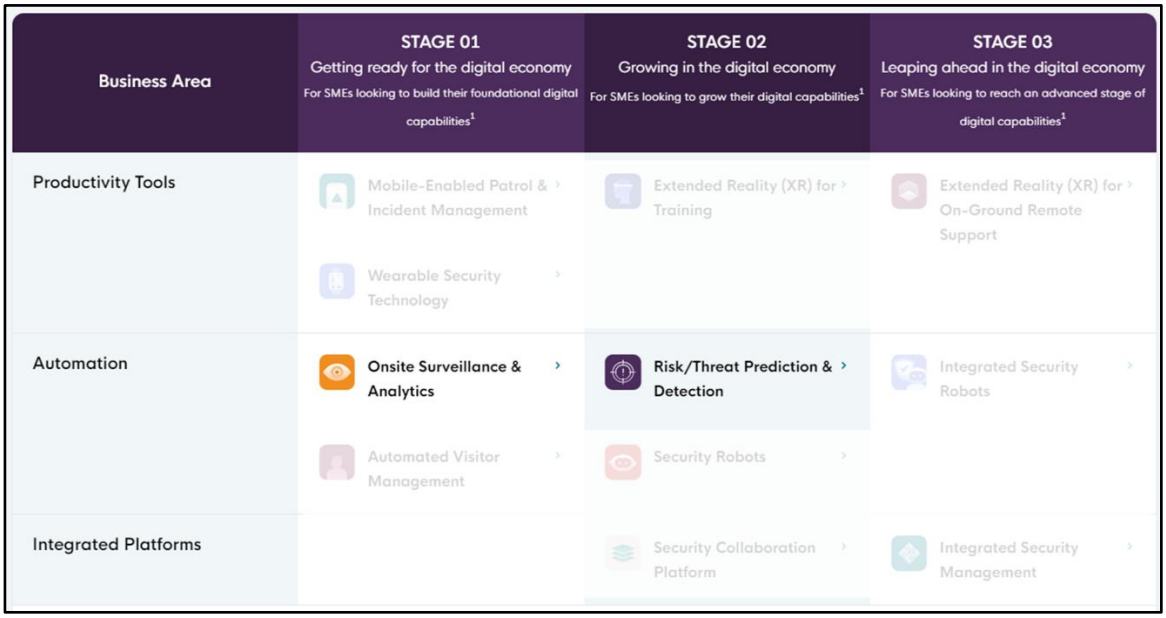


Figure 1: Snapshot of the Digital Solution Roadmap in the Security Industry Digital Plan

3.4 Based on the consultation with the Security Industry during the development of the IDP, we observed that security companies today rely mainly on "Onsite Surveillance and Analytics" ["OSA"] solution, a Stage 1 solution category in the Security Industry IDP, in their security guarding services. OSA makes use of IP-enabled video cameras augmented with analytics to detect security incidents and enhance onsite security monitoring. Typical features of OSA include:

- Object recognition and classification for identifying people, vehicles, and other objects.
- Facial recognition for identifying individuals and detecting unauthorized personnel.
- License plate recognition for monitoring vehicle movements.

3.5 Adopting OSA benefits security companies in various ways. It enhances security services, improves incident response with real-time alerts and remote monitoring, and reduces the needs for foot patrol.

3.6 Moving forward, the security industry sees an increasing need for proactive and predictive security measures, especially from stakeholders who embrace the AI-driven analytic solutions. This shift aims to move away from conventional security guarding methods and basic video analytics towards man-less guarding. The growing demand is fuelled by the desire to prevent security incidents and potential criminal activities, such as identifying intoxicated individuals loitering around building premises, detecting suspicious drowning gestures in swimming pools, or recognising aggressive behaviours towards building residents. Early intervention and proactive measures in response to these events are crucial for enhancing overall security and safety.

3.7 In addition, there is a noticeable trend among security service buyers towards outcome-based contracts (OBC), which require value-added services aimed at diminishing security incidents and events in building premises while concurrently reducing the manpower resources in guarding. This trend underscores an increasing focus on delivering tangible security outcomes and optimising resource allocation. Moreover, the emergence of advanced AI technologies presents a timely opportunity to enhance security measures in line with the OBC model.

3.8 To better address these evolving demands, it is essential to heighten awareness and promote the advanced form of OSA, referred toas the “Risk/Threat Prediction & Detection” (“RTPD”) solution, which falls under Stage 2 solution category in the Security IDP. RTPD leverages advanced AI to detect and predict potential risks and threats based on observed behaviours, gestures, or activities. The typical features of RTPD are detailed in Para 4.3 in this document. Adopting RPTD will significantly improve situational awareness of the security companies and further reduce the manpower resources needed to provide security guarding services.

3.9 This CFP aims to support the adoption of advanced RTPD solutions that can be integrated with existing OSA solutions of security companies (include existing CCTV, NVR/DVR, VMS).

4. FUNCTIONAL REQUIREMENTS

This section specifies the functional requirements of Risk/Threat Prediction and Detection ("RTPD").

RTPD should support either one of below deployment models:

a. **On-Premises & Edge Computing Deployment Model**
   This deployment model fully utilises edge devices deployment on building premises (decentralise architecture of remote surveillance) that include all edge analytics features including storages in AI box or devices.

b. **Cloud-Based and Video Analytics as a Service (VAaaS) Deployment Model**
   This deployment model fully utilises cloud infrastructure allowing end users to access video analytics capabilities remotely via the internet (centralise architecture of remote surveillance) without the need for on-premises upfront investments or technical expertise for on-premises installation.

c. **Hybrid Deployment Model**
   This deployment model performs initial processing/analysis of video data and enable real time streaming video to be stored locally while event video data (e.g. 30 seconds before and after event/incident or potential threat prediction) and metadata generated by edge devices will be transmitted to the cloud platform for further analysis/advanced analytics.

Any deployment model should be scalable, support distributed processing and horizontal scaling for efficient performance to accommodate future expansion and a growing number of video feeds, sources, and users. Please refer to Annex A for the 3 suggested deployment model for RTPD.

4.1 **[Mandatory]** RTPD must integrate with existing basic Video Analytics (VA) / Onsite Surveillance Analytics (OSA) solutions of security companies (either through existing in-built camera analytics or VA/OSA server or VMS) and several types of video feeds, including CCTV, IP-enable video camera, drone, security robot, body-worn cameras as well as support standard video formats and protocols for seamless integration.

4.2 **[Mandatory]** RTPD must have the capability to perform real-time analysis of video feeds to detect potential risks/threats and employ advanced predictive algorithms to forecast potential incidents, including aggressive/malicious behaviour/ gestures/ activities before any actual harm occurs (<u>at least three (3) use cases</u> from below risk threat detection and prediction use case references):

   a. Violence detection such as fighting, brawl, harassment, robbery, etc.
   b. Drowning.
   c. Person collapsing (e.g., slip, trip, fall) / showing distress (such as health emergency) monitoring.

d. Deviant/Suspicious gesture and behaviour (including body gesture, posture, facial expression, gaze analysis) such as loitering, observation, staring, climbing, tail gating, etc.
e. Fire and smoke (including people smoking cigarettes).
f. Negative emotions recognition such as anger, fear, anxiety, hate, regret, sadness, guilt, etc that potentially leading to incident (either self-inflicted or harm to others).
g. Abnormal Sound Detection such as screams, explosions, or alarms, triggering immediate alerts for security personnel to investigate.
h. Other proposed use cases (subject to further assessment and approval).

4.3 **[Mandatory]** RTPD must provide real time alerts and notifications (e.g. RTPD platform alert/ alarm, SMS, email, mobile apps, or other push notification) upon detecting potential risks or threats. The alert should also contain recommended action of mitigation measurement (e.g., immediate deployment of resources to manage incident detected).

4.4 **[Mandatory]** RTPD must provide interface for management dashboard such as top threat prediction, common incident, accuracy level including operational dashboard such as real time live video and audio stream monitoring, historical playback of video feeds, system configuration, and reinforcement feedback loops for retrain video analytics model. This includes cross-filtering feature on the dashboard(s) to allow users analyse data and generate insights to make informed decisions.

4.5 **[Mandatory]** RTPD must provide strict access controls in place to ensure that only authorised users can access the recorded footage, including measures such as Multi-Factor Authentication (MFA) and role-based access controls.

4.6 **[Mandatory]** RTPD must provide backup features that perform regular and automated backup to another location separate from the operating environment, such as cloud back up.

4.7 **[Mandatory]** RTPD must comply with IMDA's Personal Data Protection requirements such as:
a. Features that allow for access of an individual's video footage.
b. Features to set retention periods for the video footage and flag out records which have reached the end of their retention period.
c. Encryption of personal data both for data in transit (e.g. TLS and at rest (e.g. data stored on the servers).
d. 2-Factor authentication (2FA)/Multi-Factor Authentication (MFA) to ensure that only authorised users can access personal data.

4.8 **[Optional]** RTPD should have the capability to perform video review and generate summary & detail video insight as part of post video forensic analysis to reduce response time of security threats while increasing safety and optimizing operations.

4.9 **[Optional]** RTPD should utilise audio/sound analytics to complement risk threat detection and prediction in the nearby areas that are not covered by CCTV/IP-enabled camera such as scream, cry, distress, loudness vulgarity in multi-language including local slank/Singlish.

4.10 **[Optional]** RTPD should provide reporting feature that generate comprehensive reports on detected incidents, potential risks/threats in a user-friendly and actionable manner (e.g., potential security threat based on history data and real time suspicious behaviour with recommended action).

4.11 **[Optional]** RTPD should integrate seamlessly with existing security systems, such as access control systems, visitor management system, carpark management system, alarms, incident management, Security Collaboration Platform (SCP) and/or Integrated Security Management (ISM) platform. The integration (data ingestion and outgoing push) can be via HTTPS for video metadata or Secure Real-time Transport Protocol (Secure RTP) for interoperability with third party platforms.

4.12 **[Optional]** RTPD should enhance the quality of video content or restore degraded video footage by denoise noisy videos, upscale low-resolution videos, or fill in missing frames to improve the overall visual quality and usability of video data.

4.13 **[Optional]** RTPD should provide search for specific objects, events, or patterns of interest to efficiently locate relevant segments of video data that match the search criteria and enable content-based retrieval as well as similarity search for more intuitive and effective video search capabilities (for example: facial search, search suspicious behaviour for group of people that wear red shirt at midnight, other use cases).

5 PROPOSAL SUBMISSION

5.1 Please submit the required details and documentations in this RTPD Registration to indicate your interest to participate in this CFP latest by **2 August 2024**.

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;

5.1.3 Each participant must have engaged at least 3 security agencies prospect that has expressed interest (at least 3 Letter of Interests/ LOIs) to adopt the proposed solution and 1 live demonstration session with your security agency/ security service buyer prospect to validate solution accuracy and demand awareness will be required during evaluation stage; and

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

5.2 While vendors who fulfil all mandatory requirements will be considered, it should be noted that meeting these requirements does not guarantee automatic qualification. In the situation where the numbers of vendors meeting the mandatory requirements are more than our capacity to support, then the submissions will be assessed further using the criteria outlined under clause 5.3.

5.3 For this CFP, your submission will be ranked and assessed based on the following evaluation criteria:

5.3.1 Financial soundness.
5.3.2 Ability to acquire customers.
5.3.3 Awards and Recognition.
5.3.4 Track records in delivering the proposed solution with similar scope.
5.3.5 Cost-effectiveness.
5.3.6 Number of optional requirements met.
5.3.7 Ease of use and Rollout deployment timeline.
5.3.8 Accuracy of the Video Analytics.

5.4 The supportable qualifying cost only cover RTPD solutions (software license or subscription cost, RTPD servers and professional services). It won't cover new/ existing CCTV cameras, NVR/DVR, Video Gateway, and VMS.

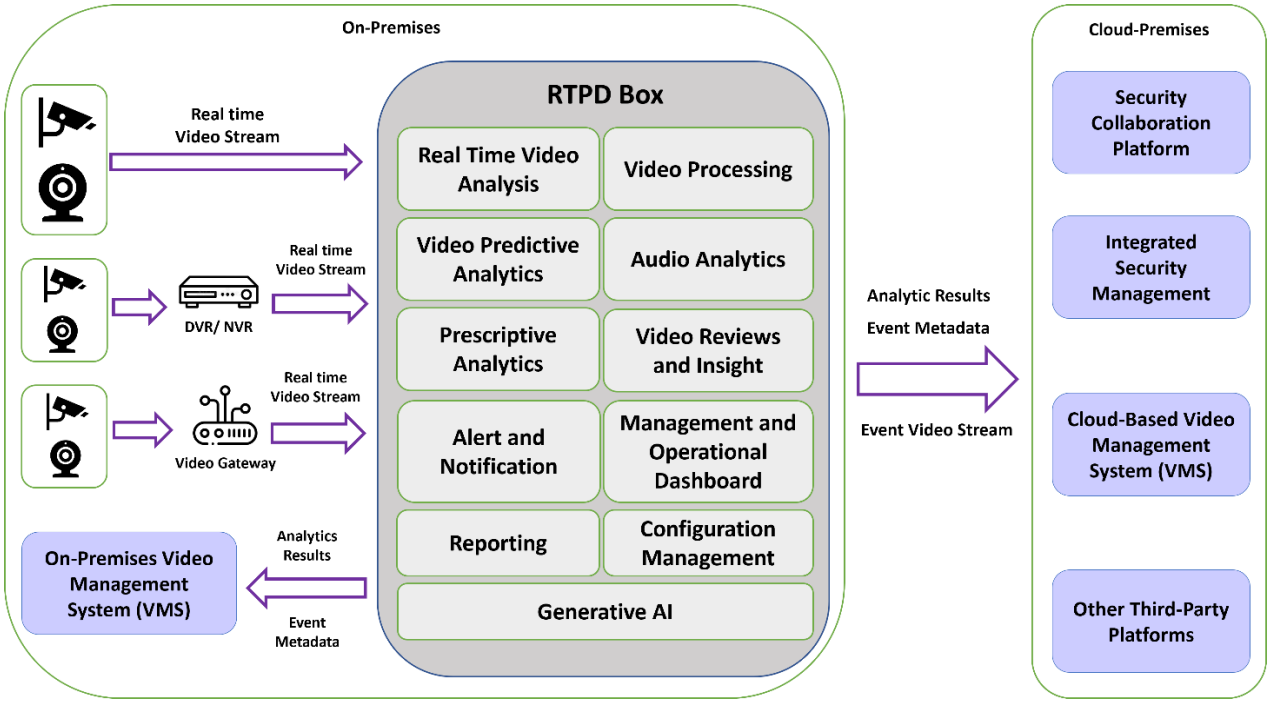
5.5 IMDA reserves the right to make the final decision on the proposal approval. If your proposal is approved, you will be notified by IMDA within 4-6 months from submission date.

[End of Document]

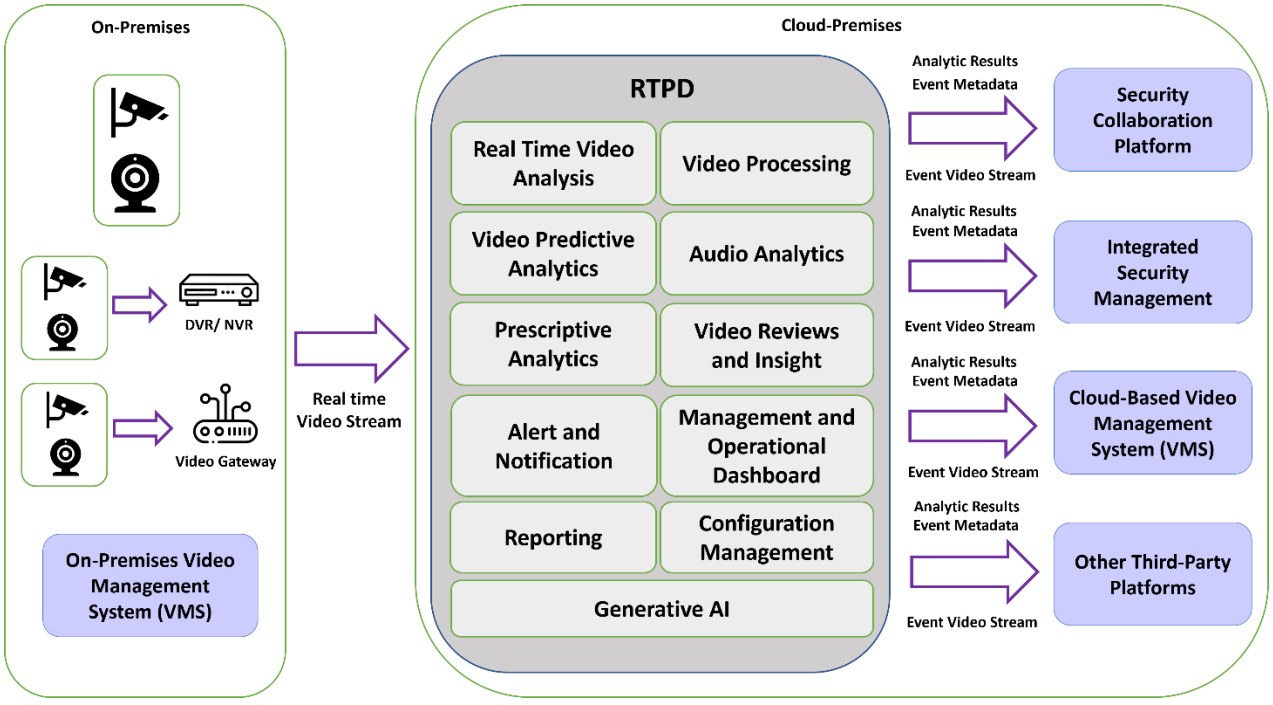
Annex A (Suggested RTPD Solution Deployment Model)

The diagrams below illustrate the suggested deployment models of the Risk/Threat Prediction and Detection Solution:

Model A: On-Premises & Edge Computing Deployment



Model B: Cloud-Based and Video Analytics as a Service (VAaaS) Deployment



Model C: Hybrid Deployment Model