Technology, Media & Telecommunications

Public Consultation on Proposed Guidelines to Secure AI Systems

Introduction

Artificial Intelligence ("**AI**") has been widely recognised and adopted for its potential to drive efficiency and innovation across all sectors. However, certain inherent threats stand in the way of the achievement of such potential. AI systems can be vulnerable to cyber security risks such as adversarial attacks, where malicious actors intentionally manipulate or deceive the AI system, as well as the exacerbation of existing risks to enterprise systems. This could result in data leakage or data breaches, or harmful and unfair model outcomes.

Securing AI systems should thus be a priority for enterprises seeking to develop or deploy AI solutions. But with AI security still being a developing field of work, and with an array of evolving threats across all stages of the AI lifecycle, the process of securing AI systems may seem daunting.

To address this, the Cyber Security Agency of Singapore ("**CSA**") has developed the Guidelines on Securing AI Systems ("**Guidelines**") to help system owners secure AI throughout its lifecycle. The Guidelines aim to provide evergreen principles to raise awareness of threats that could compromise AI behaviour and system security, and guide system owners on implementation of security controls and best practices to protect AI systems against potential risks.

CSA is also working with AI and cybersecurity practitioners to develop a Companion Guide for Securing AI Systems ("**Companion Guide**"). This is a community-driven resource to complement the Guidelines, compiling practical measures and controls, and drawing from industry and academia.

CSA is conducting a public consultation on the Guidelines and the Companion Guide. The consultation closes on 15 September 2024.

This Update provides a summary of the Guidelines and highlights the key features. Organisations wishing to provide feedback on the Guidelines and the Companion Guide should feel free to contact our team for guidance in this regard.

Understanding AI Threats

Securing an AI system may present markedly different challenges from traditional IT systems. The Guidelines highlight the cybersecurity risks associated with AI, including classical cybersecurity risks as well as novel attacks such as Adversarial Machine Learning ("**ML**") that set out to distort the model's behaviour to produce inaccurate, biased, or harmful output.

Classical cybersecurity risks:

(a) Supply chain attacks.

(b) Intrusion or unauthorised access.

(c) Disruptions to cloud services, data centre operations, or other digital infrastructure (e.g. through Denial of Service attacks).

Adversarial ML:

(a) Data poisoning (injecting malicious or corrupted data into training data sets).

(b) Evasion attacks (on trained models) to distort outcomes.

(c) Inference attacks or extraction attacks (probing the model) to expose sensitive or restricted data, or to steal the model.

Risk Assessment

The Guidelines propose starting the process of securing AI systems with a risk assessment to enable organisations to identify potential risks, priorities, and subsequently, the appropriate risk management strategies. The Guidelines recommend a four-step risk process:

(a) **Step 1**: Conduct risk assessment, focusing on security risks to AI systems.

(b) **Step 2**: Prioritise areas to address based on risk/impact/resources.

(c) **Step 3**: Identify and implement the relevant actions to secure the AI system.

(d) **Step 4**: Evaluate residual risks for mitigation or acceptance.

Guidelines for Securing AI Systems

The Guidelines apply across the five lifecycle stages of the AI system. System owners should read these as key issues to consider in securing their adoption of AI.

(a) **Stage 1: Planning and design**

- Raise awareness and competency on security risks.
- Conduct security risk assessments.

(b) **Stage 2: Development**

- Secure the supply chain.
- Consider security benefits and trade-offs when selecting the appropriate model to use.
- Identify, track and protect AI-related assets.
- Secure the AI development environment.

(c) **Stage 3: Deployment**

- Secure the deployment infrastructure and environment of AI systems.
- Establish incident management procedures.
- Release AI systems responsibly.

(d) **Stage 4: Operations and maintenance**

- Monitor AI system inputs.
- Monitor AI system outputs and behaviour.
- Adopt a secure-by-design approach to updates and continuous learning.
- Establish a vulnerability disclosure process.

(e) **Stage 5: End of life**

- Ensure proper data and model disposal.

Concluding Words

The Guidelines are designed to support AI system owners in securing their adoption of AI solutions. The Guidelines identify potential security risks associated with the use of AI and set out guidelines for mitigating security risks at each stage of the AI lifecycle.

Organisations should familiarise themselves with the principles and guidance set out in the Guidelines to provide direction in the use of AI solutions. Stakeholders should also assess the Guidelines for issues of adequacy, clarity, and practicality, and submit the relevant feedback to CSA as part of the consultation process.

If you have a query on the Guidelines or the Companion Guide, or if you wish to provide feedback under the consultation, please feel free to contact our team. Our Technology, Media and Telecommunications team at Rajah & Tann will be able to assist in any legal issues, while the team at Rajah & Tann Technologies and Rajah & Tann Cybersecurity will be able to assist in technological and cybersecurity issues.

Technology, Media & Telecommunications

Contacts

Rajesh Sreenivasan
Head, Technology, Media & Telecommunications

T +65 6232 0751

rajesh@rajahtann.com

Steve Tan
Deputy Head, Technology, Media & Telecommunications

T +65 6232 0786

steve.tan@rajahtann.com

Benjamin Cheong
Deputy Head, Technology, Media & Telecommunications

T +65 6232 0738

benjamin.cheong@rajahtann.com

Click **here** for our Partners in our Technology, Media and Telecommunications Practice.

Rajah & Tann Technologies

Raymond Lum
Chief Executive Officer
Rajah & Tann Technologies

T +65 6988 4903

raymond.lum@rttechlaw.com

Rajah & Tann Cybersecurity

Wong Onn Chee
Chief Executive Officer
Rajah & Tann Cybersecurity

T +65 6996 0404

onnchee@rtcyber.com

Please feel free to also contact Knowledge Management at eOASIS@rajahtann.com

Our Regional Contacts

RAJAH & TANN SOK & HENG | *Cambodia*
Rajah & Tann Sok & Heng Law Office
T +855 23 963 112 / 113
F +855 23 963 116
kh.rajahtannasia.com

RAJAH & TANN 立杰上海
SHANGHAI REPRESENTATIVE OFFICE | *China*
Rajah & Tann Singapore LLP
Shanghai Representative Office
T +86 21 6120 8818
F +86 21 6120 8820
cn.rajahtannasia.com

ASSEGAF HAMZAH & PARTNERS | *Indonesia*
Assegaf Hamzah & Partners

Jakarta Office
T +62 21 2555 7800
F +62 21 2555 7899

Surabaya Office
T +62 31 5116 4550
F +62 31 5116 4560
www.ahp.co.id

RAJAH & TANN | *Lao PDR*
Rajah & Tann (Laos) Co., Ltd.
T +856 21 454 239
F +856 21 285 261
la.rajahtannasia.com

CHRISTOPHER & LEE ONG | *Malaysia*
Christopher & Lee Ong
T +60 3 2273 1919
F +60 3 2273 8310
www.christopherleeong.com

RAJAH & TANN | *Myanmar*
Rajah & Tann Myanmar Company Limited
T +95 1 9345 343 / +95 1 9345 346
F +95 1 9345 348
mm.rajahtannasia.com

GATMAYTAN YAP PATACSIL GUTIERREZ & PROTACIO (C&G LAW) | *Philippines*
Gatmaytan Yap Patacsil Gutierrez & Protacio (C&G Law)
T +632 8894 0377 to 79 / +632 8894 4931 to 32
F +632 8552 1977 to 78
www.cagatlaw.com

RAJAH & TANN | *Singapore*
Rajah & Tann Singapore LLP
T +65 6535 3600
sg.rajahtannasia.com

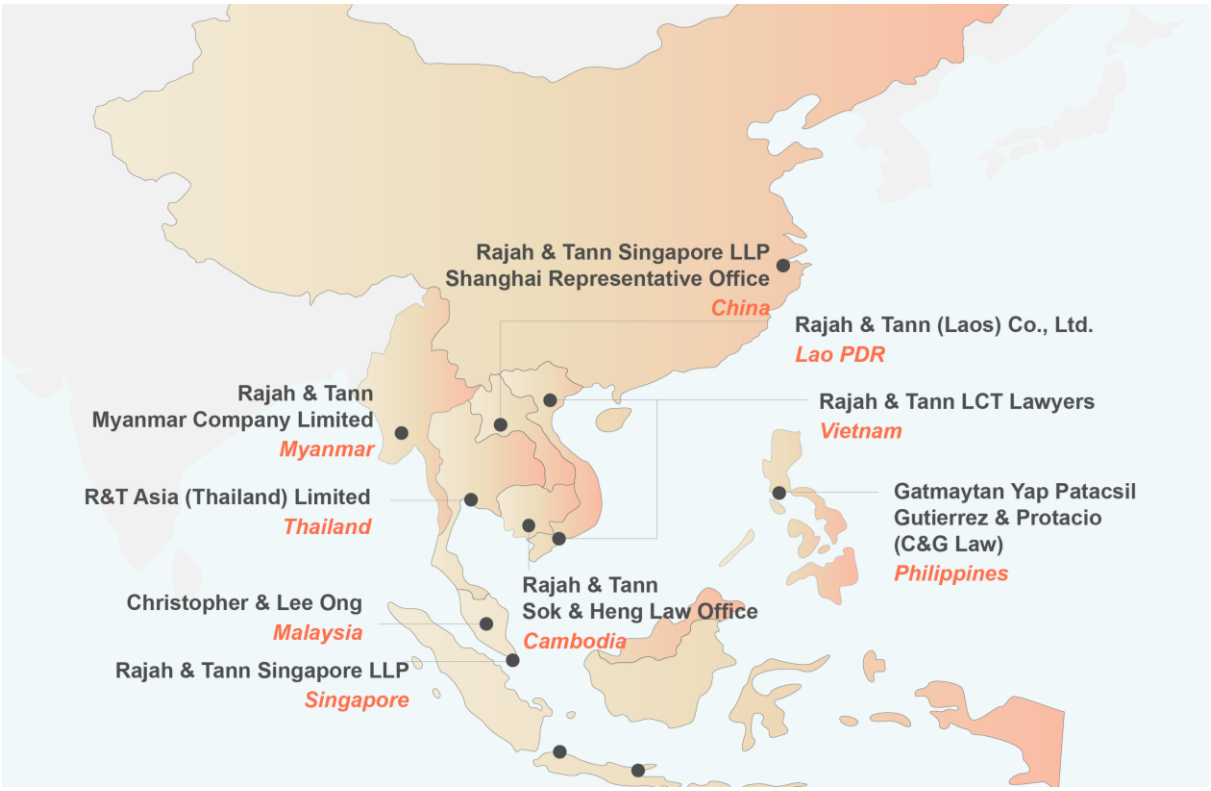
RAJAH & TANN | *Thailand*
R&T Asia (Thailand) Limited
T +66 2 656 1991
F +66 2 656 0833
th.rajahtannasia.com

RAJAH & TANN LCT LAWYERS | *Vietnam*
Rajah & Tann LCT Lawyers

Ho Chi Minh City Office
T +84 28 3821 2382 / +84 28 3821 2673
F +84 28 3520 8206

Hanoi Office
T +84 24 3267 6127
F +84 24 3267 6128
www.rajahtannlct.com

Our Regional Presence



Rajah & Tann Singapore LLP is one of the largest full-service law firms in Singapore, providing high quality advice to an impressive list of clients. We place strong emphasis on promptness, accessibility and reliability in dealing with clients. At the same time, the firm strives towards a practical yet creative approach in dealing with business and commercial problems. As the Singapore member firm of the Lex Mundi Network, we are able to offer access to excellent legal expertise in more than 100 countries.

Rajah & Tann Singapore LLP is part of Rajah & Tann Asia, a network of local law firms in Cambodia, China, Indonesia, Lao PDR, Malaysia, Myanmar, the Philippines, Singapore, Thailand and Vietnam. Our Asian network also includes regional desks focused on Brunei, Japan and South Asia.