Response to the Cyber Security Agency of Singapore (CSA) Public Consultation Feedback on the Securing Agentic AI - An Addendum to the Guidelines and Companion Guide on Securing AI Systems

From the American Chamber of Commerce in Singapore
30 December 2025

Contact:
Qiao Mei Lee
Head, Committees
qmlee@amcham.com.sg
1 Scotts Road, #23-03/04/05
Shaw Centre Singapore 228208

30 Dec 2025

Mr David Koh
CEO
CSA Singapore
5 Maxwell Road, MND Complex
Tower Block #02-00, #03-00
Singapore 069110

Re: Feedback on the Securing Agentic AI - An Addendum to the Guidelines and Companion Guide on Securing AI Systems

The American Chamber of Commerce in Singapore (AmChamSG) welcomes the opportunity to provide input to the Cyber Security Agency of Singapore (CSA).

AmChamSG is the largest and most active international business association in Singapore and Southeast Asia, with over 7,000 members representing nearly 650 companies. Many U.S. companies establish their regional headquarters in Singapore before scaling up and expanding in the region. Our goal is to meet present and future challenges to the mutual benefit of American business and the people of Singapore.

AmChamSG's feedback on the Securing Agentic AI - An Addendum to the Guidelines and Companion Guide on Securing AI Systems ("Addendum") follows:

1. In the first instance, we would like to commend CSA on releasing this Addendum. We value the explicit confirmation that the Addendum is an informational supplement to the existing Guidelines and is not intended as a mandatory implementation document.

2. We appreciate that the Addendum takes a risk-based approach towards the AI development life cycle, which is an appropriate and necessary approach to take for evolving and frontier technologies like agentic AI. We also value that the Addendum is tailored to agentic architectures, focusing on their unique capabilities and abilities. The inclusion of practical scenarios and case studies effectively illustrates the application of risks and controls.

3. We believe that the Addendum will be an effective resource for organizations seeking to select appropriate controls, particularly with the added concepts of taint-tracing, illustrated mapping of workflows and associated risks.

AmChamSG submits the following suggestions and requests for clarification for the CSA's further consideration:

4. In the case of taint-tracing (p26), we seek guidance on the specific measures and mechanisms recommended for identifying 'tainted flows' without unnecessarily increasing the burden to implement entirely new, resource-intensive systems. The guidance should consider defining or providing some pointers to define contextual trust, criticality for each enterprise as it may vary between industries, size, and other factors.

5. Related, we would like to understand the controls and processes that the industry is expected to implement to detect these tainted data flows, trace these flows throughout the life of the system, and the relative importance to be assigned to these controls within the overall security framework.

6. Regarding OWASP threat T10 Overwhelming Human In the Loop, while the goal of "ensuring adequate human oversight" (p48) is appropriate, we recommend that CSA provides more comprehensive guidance:
    a. Further guidance on how organisations can determine what is “adequate” particularly in the context of irreversible (high-risk) system decisions.
    b. Specific guidance on how to apply human oversight controls for automated agentic AI systems, particularly given the speed of agent-driven decisions, and
    c. Explore examples of risk mitigation strategies, such as the establishment of periodic penetration testing regimes, to ensure that systemic risks are measured and assessed regularly, especially following changes in application or development versions.

7. We propose a suggestion to enhance the current framework by recommending the use of supply chain policy (p32) to identify these agentic workflows. We can also lean on existing data protection guidelines, to balance the need to define boundaries of trust without introducing overly prescriptive mandates e.g. suggesting that a data classification approach be put in place, or using an existing trust framework to identify and establish trust markers.

8. Concerning the disclosure of sensitive information and Personally Identifiable Information (PII) (p85), we acknowledge that these concepts intersect with existing data protection, privacy, and AI regulations. We recommend that the CSA develops a deeper dive on applying these concepts practically for agentic systems:
    a. Providing guidance on how to align these requirements with existing cyber trust certifications rather than establishing new requirements for agentic AI, or
    b. Developing material on how to contextualise the risks associated with PII specifically within the agentic AI scenarios.

9. We appreciate that the agentic AI landscape is changing rapidly and recognize the value of including Agent Communication Protocol (ACP) and Agent Network Protocol (ANP). These provide a more complete view of established protocols that complement MCP and A2A, helping organizations develop and secure agentic AI solutions.

10. We value the comprehensive list of threats provided and recognize that the complexity of agentic AI necessitates explicitly reinforcing a strong AI governance framework within this addendum. While the need for governance is addressed in the companion guide, referencing ISO 42001 would provide a globally recognized benchmark for risk management and compliance. This addition ensures that agentic deployments are consistently documented, evaluated, and reported across the industry

AmChamSG greatly values the CSA’s efforts in engaging industry stakeholders through open dialogue. We look forward to collaborating further to advance Singapore’s AI strategy.

Yours Sincerely,

Hsien-Hsien Lei

Dr. Hsien-Hsien Lei
Chief Executive Officer