Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Artificial intelligence and machine learning: Supply chain risks and mitigations

Co-seal changes

Last updated: March 2026

Summary

Adopting artificial intelligence (AI) and machine learning (ML) systems introduces unique supply chain risks, which can threaten the cyber security of an organisation if not securely managed. It is crucial that organisations understand the risks and how to mitigate them when developing or incorporating AI and ML into their systems.

This document provides a summary of the changes introduced in the March 2026 update to the *Artificial intelligence and machine learning: Supply chain risks and mitigations* publication.

This update includes revision and expansion of the original publication in collaboration with co-sealing agencies, including:

- Canadian Centre for Cyber Security (Cyber Centre)
- Singapore Cyber Security Agency (CSA)
- Republic of Korea National Intelligence Service (NIS)
- Japan National Cybersecurity Office (NCO)
- New Zealand National Cyber Security Centre (NCSC-NZ)
- United Kingdom National Cyber Security Centre (NCSC-UK)
- United States National Security Agency (NSA).

The revised guidance incorporates expanded explanations, clarification of existing content and new sections addressing additional risk management and mitigation concerns.

Key additions include guidance on how organisations might:

- revise their risk management when incorporating AI and ML systems
- quarantine and test AI data before use in internal environments
- test performance to verify that ML models behave as expected.

The overall structure remains largely consistent with the original version, with expanded guidance that better aligns with international best practices for AI and ML supply chain security.

Significant changes list

Section	Change type	Details
Introduction	Change	Clarifications
Supply chain risk management concepts for AI and machine learning	Change	Clarified and added more details to existing sections
Supply chain risk management concepts for AI and machine learning	Added	Added new sections: • *Supply chain integrity assessments* • *Revise risk management*
AI data: Mitigations	Added	Added a new section: • *Quarantine and testing*
Machine learning models: Mitigations	Change	Improved explanation for sections: • *Trusted and transparent sources* • *Model explainability and transparency* • *Input-output monitoring* • *Security tools*
Machine learning models: Mitigations	Added	Added a new section: • *Performance testing*
AI software: Mitigations	Change	Improved general mitigations explanation
More information	Added	Added additional relevant links for partner publications

Disclaimer

The material in this guide is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances.

The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

Copyright

Use of the Coat of Arms

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian Cyber Security Centre