Corresponding essay: **E10** “The Supply Chain You Cannot See”

ADMISSION CONTROL FOR INSTRUCTION-BEARING COMPONENTS

The 4P Gate

Pick one component you installed in the last thirty days, list every component that can speak to your agent as instruction, then run the chosen one through the four gates.

BRING One tool, skill, MCP server or config you admitted recently

Agent Instruction BOM

List every component that can speak to your agent as instruction, not just the code it runs. If the list surprises you, that is the finding.

Component and exact version	Type (prompt / skill / MCP server / tool description / manifest / remote prompt URL / mutable config)	Source and owner	Can it change after approval?

Run one component through the 4P Gate

Take one entry from the inventory above. Mark each gate Pass or Block. Any honest "no", or "we do not know", is a stop sign. Re-run on update and on any permission or pull-direction change.

1 Provenance

Who produced this exact version, who reviewed the description the model sees, and can the version be verified? Block on an unknown maintainer, an unsigned or unpinned package, or a silent registry or config swap.

☐ Pass ☐ Block

2 Permissions

What can it reach on load or execution if it is compromised? Block on default access to filesystem, secrets, network, shell, production data or other tools. Pass on least privilege and a scoped boundary.

☐ Pass ☐ Block

3 Posture

What scanner or review actually touched it, including a hidden-text check? Block with no scan, no config-diff review and no exfiltration-pattern review.

☐ Pass ☐ Block

4 Pull-direction

Can it fetch new instructions, commands or config after approval? Block on runtime URLs, mutable remote prompts, command fields from config or uncontrolled updates.

☐ Pass ☐ Block

GATE VERDICT, WHICH P BLOCKS FIRST, AND WHO OWNS THAT BLOCK

If you override a failed gate

A failed gate may be overridden only with all four fields written down. An override missing any of them is the supply-chain failure already in progress.

Override field	Your answer
Named owner - a person, not a team, accountable for the decision	
Risk tier - how much authority the component holds	
Expiry date - when this temporary exception ends	
Rollback plan - how the component is removed and what is restored	

Companion worksheet to **Essay 10 · The Supply Chain You Cannot See**, in the series **Architecting the AI Coworker**. · Dr Peter McCann Strain · Fill this in against one real agent, action class or vendor.

Series Companion + all 22 worksheets: **Release_v12/Series_Companion.pdf**