NCCoE Workshop on Cyber Supply Chain Risk Management

Jim Mann
Office of the Chief Engineer
HP Inc.
September 10, 2019

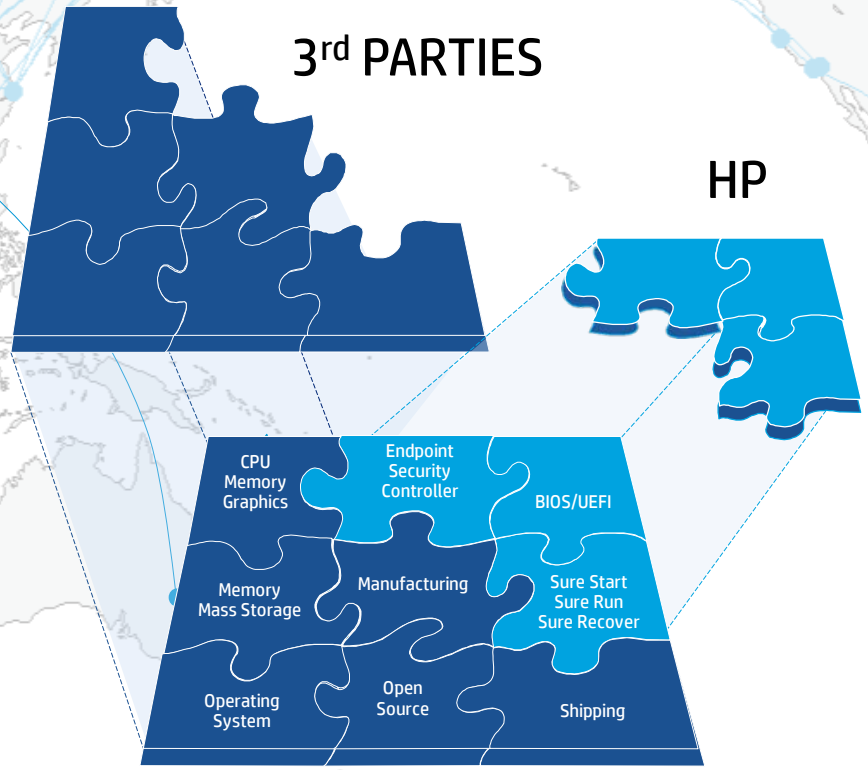
Increased scrutiny on supply chain security

Arguably the most active area in cybersecurity right now

- Some real issues, some FUD
- Worldwide
- Customer concerns, requirements
  - Governments
  - Defense
  - Enterprise/Commercial customers
  - Verticals: Healthcare, Financial, Energy, Automotive, Aerospace, Insurance
- Regulatory and legislative activity
- Standards activity

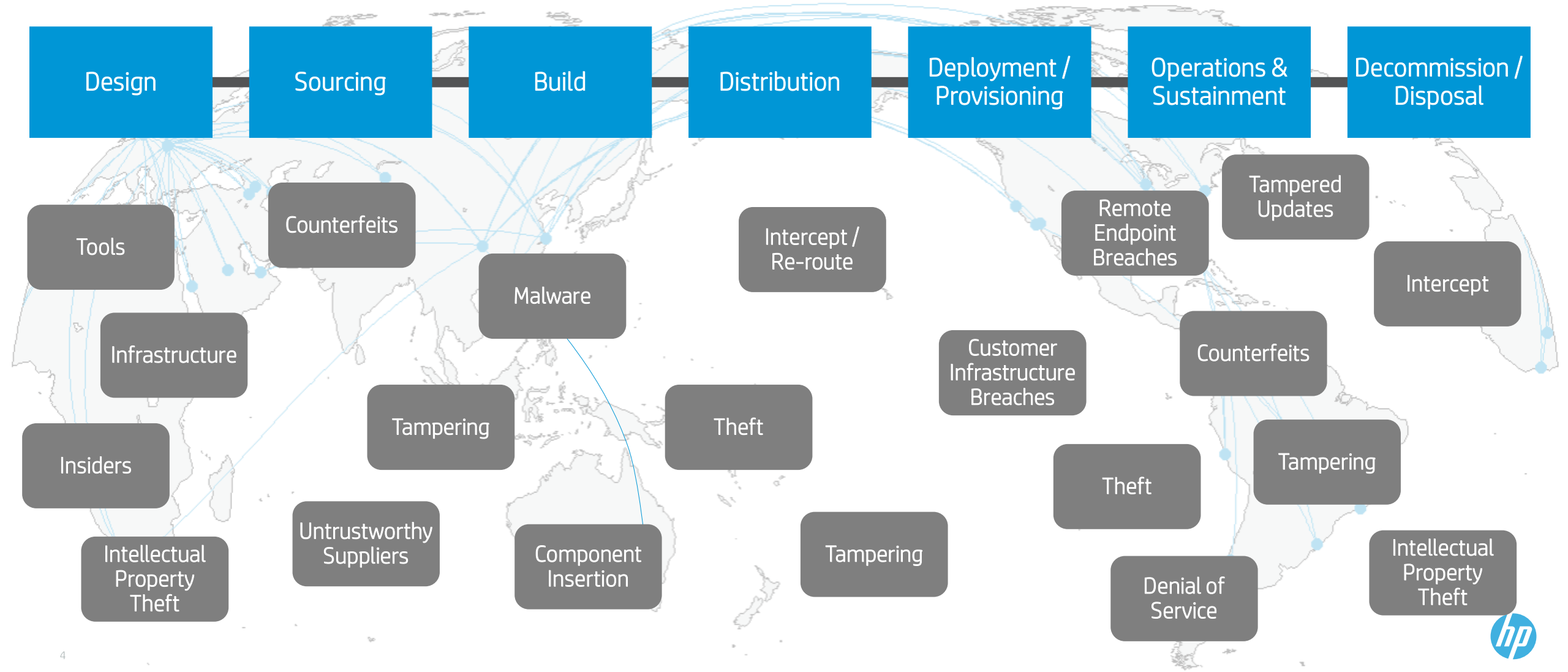
The ICT supply chain is long and complex

Design | Sourcing | Build | Distribution | Deployment / Provisioning | Operations & Sustainment | Decommission / Disposal



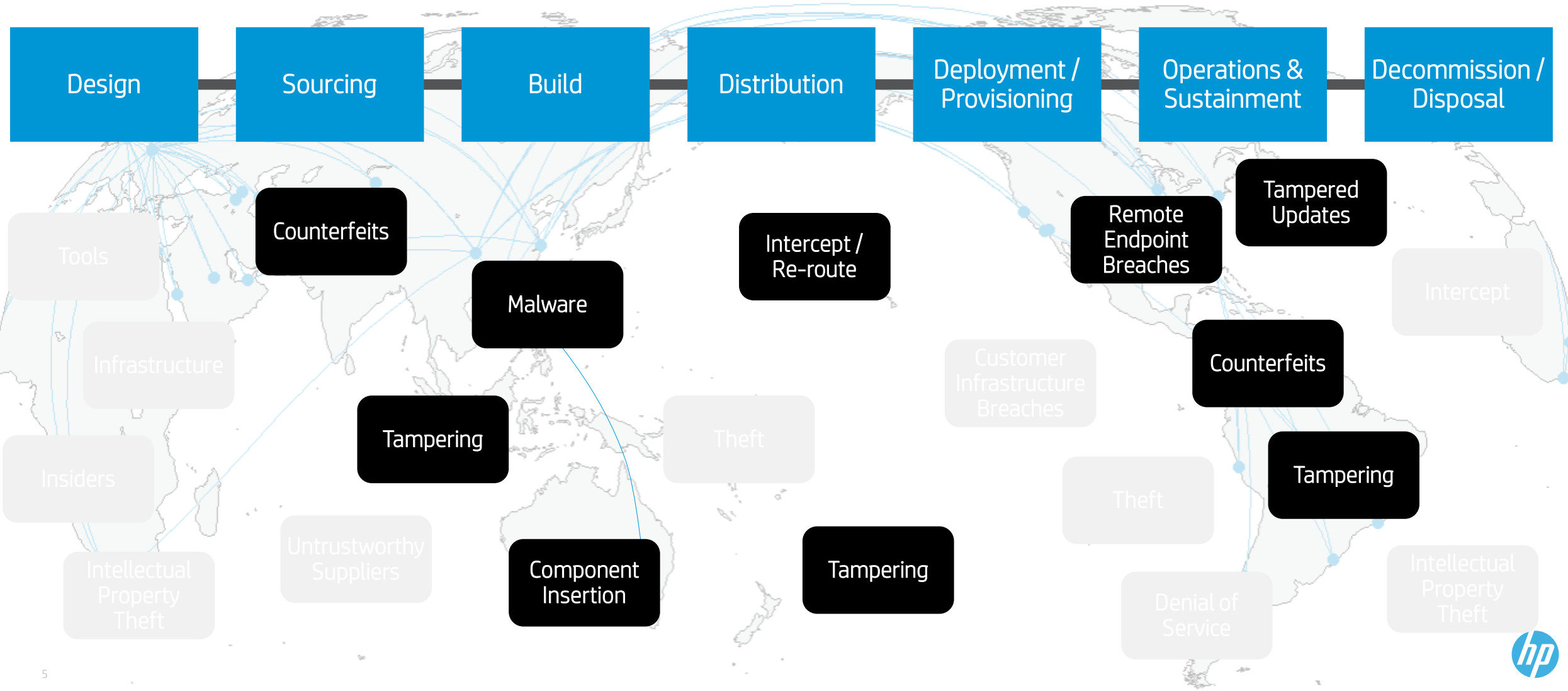
ICT Supply Chain Risks

[Not a necessarily comprehensive list]



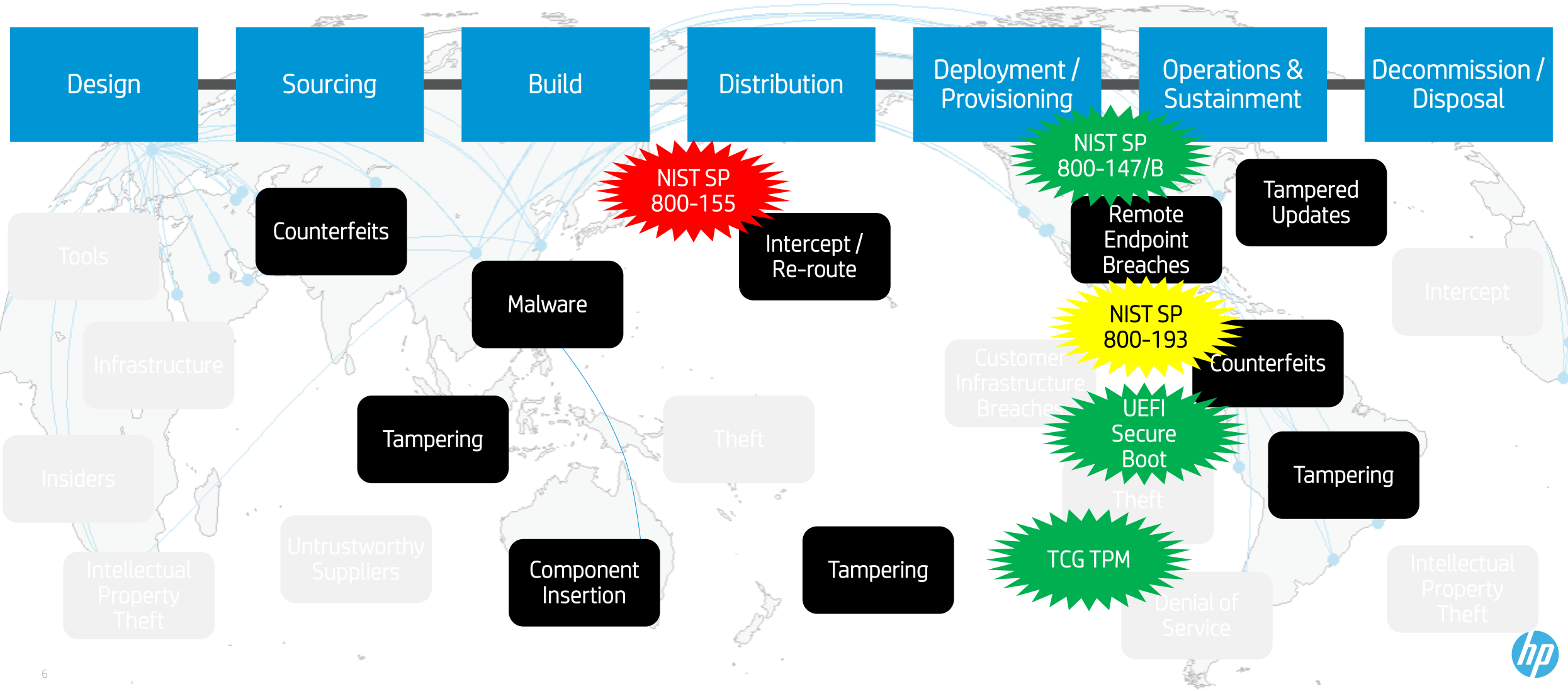
ICT Supply Chain Risks (in Scope for NCCoE Project)

[Not a necessarily comprehensive list]

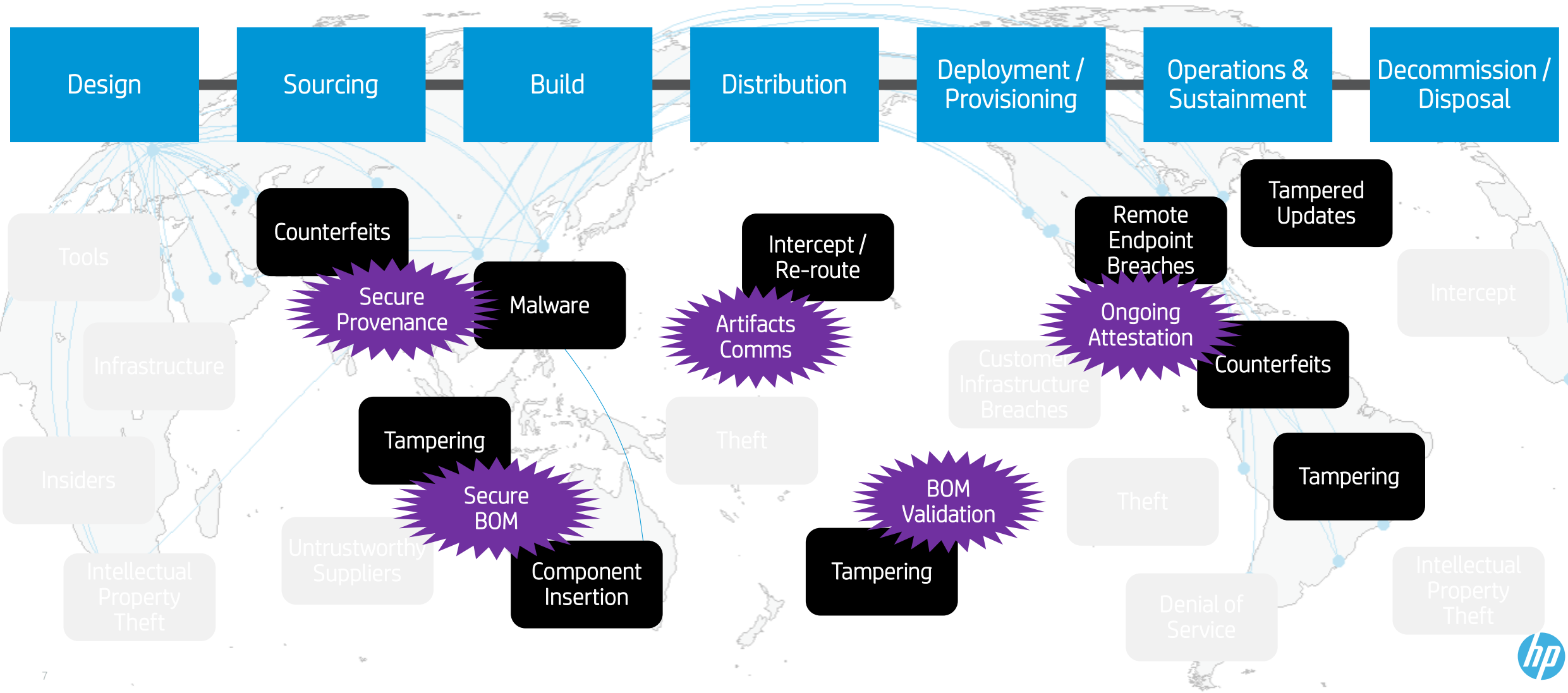


Some Existing Technical Mitigations Based on Industry Standards

[Not a necessarily comprehensive list]



NCCoE Project Opportunities



Standards-based Innovation

- Solutions should be founded in industry standards
  - Industry Consortia (TCG, UEFI, Global Platform, …)
  - Standards Developing Organizations (NIST, ISO, ETSI, …)
  - Public-private forums (NTIA, …)
  - Open forums (IETF, …)
- ICT providers should be free to innovate, and compete, on top of standards