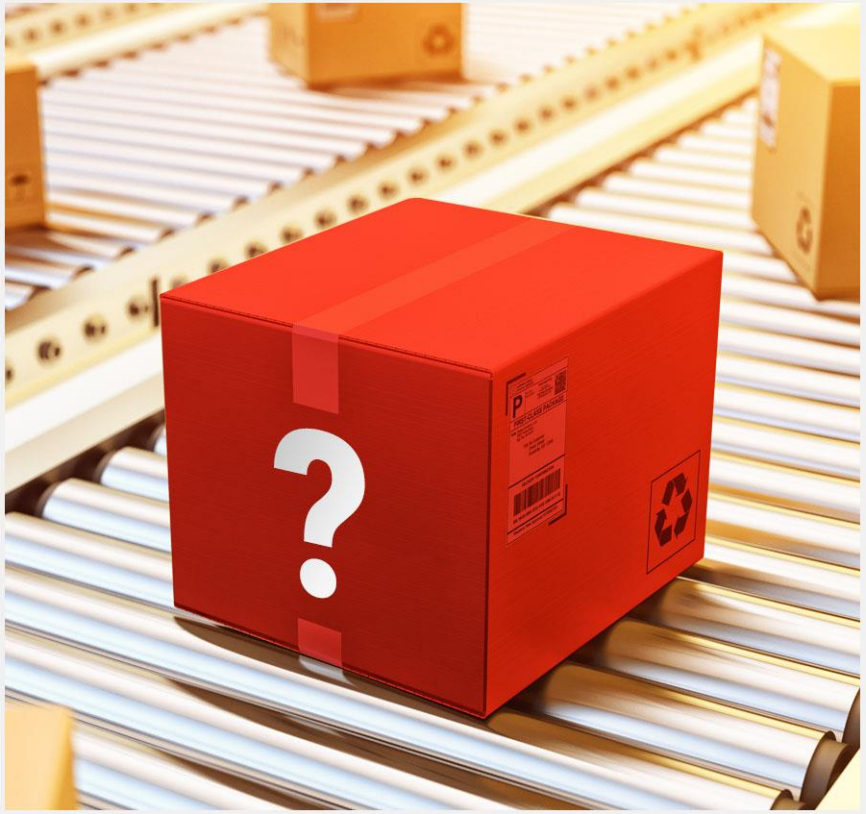
Common Sense & Common Good in the Supply Chain

John Loucaides, September 2019

Maybe It’s Time to Question Some Assumptions ...

- **How big is this industry again?**
  There must be conflicting goals.
- **Do you know your dependencies?**
  There must be something changing about them.
- **Can we keep up with all this and do our jobs?**



Help Us Help You Help Them

Disproportionately help defense by enabling others to secure their systems ...

- Enable additive security—“plugins” to enforce policies
- Enable integrity checks—“plugins” to observe/measure
- Enable trusted sources—how do we know it is “official”?

Maybe We're on the Right Track...

Open Communities & Sharing

- Code (Tianocore, Coreboot, etc)
- Measurements & Updates (LVFS)
- Security Advisories
- Testing (CHIPSEC, HBFA, etc)

Next? Making it easier...

- Published Measurements
  - Hashes
  - Behaviors
  - Status / config
- Integrity Interfaces
  - Read the measurements
- Policy plugins