Hewlett Packard
Enterprise

10th September 2019

Secure Manufacturing Considerations

CJ Coppersmith

Seismic changes

- Regulatory Motions
  - Sec. 301 tariff landscape disfavors PRC
  - Executive Order on Securing the ICT and Services Supply Chain
  - DHS ICT Supply Chain Risk Management Task Force
  - DoD Tech Sector Industrial Base Task Force
  - S. 3085 Federal Acquisition Supply Chain Security Act of 2018.
  - EO 13806 - Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States
  - Federal Information Technology Supply Chain Risk Management Improvement Act of 2018
  - NDAA Section 806
  - Mattis Moves to Protect Defense Supply Chain From Rivals' Theft
  - Supply Chain Act of 2018
- Threats
- **Counterfeiting**
- **Software implants**
- **Firmware implants**
- **Hardware implants**
- **Malware**
- **IP theft**
- Industry Trends
  - General industry trajectory due to reported and actual incidents
    - Bloomberg Allegations (October 2018)
    - Trusted Computing Group Platform Certificates (industry standard)
    - DMTF Security Protocol and Data Model (industry standard)
    - NIST supply assurance project
  - Customer Interest

Secure Manufacturing Considerations

– Considerations

- **Each component attests to its own integrity?**
- **Each system attests to its own composition?**
- **System and component traceability?**
- **Augmented by**
  - HW Root of Trust, NIST SP800-193
  - Deep Supply Chain Risk Management

– Capabilities

- **IEEE.802.1AR DevID certificates**
- **TCG platform certificate support**
- **Block chain security**
- **Signed as-built manifest**

Secure Manufacturing Ecosystem

– Cryptographic component information

– Marshalled to platform certificate

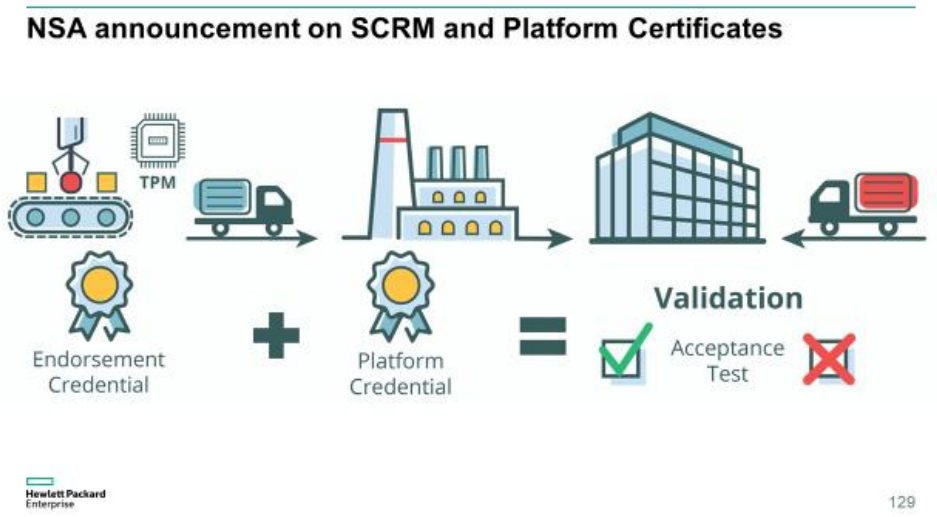
– IDEVID as authentication predicate

– Secure Recordation

– HW Root of Trust

– Platform Resilience

– Strong SCRM Basis



Hewlett Packard
Enterprise

Thank you