Global context

- Increasing country-level concern about cybersecurity threat from potentially unfriendly foreign powers

- Advanced infrastructure technologies for
    - Power generation (e.g. nuclear plants)
    - Power distribution
    - Information networks (e.g. 5G)

- Potential for spying, disruption, sabotage

- Five Eyes intelligence alliance
    - USA, Australia, New Zealand: rejected foreign influence
    - Canada: foreign influence under review
    - UK: foreign influence in place…

Background

Bloomberg: "The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies"

- "The attack by Chinese spies reached almost 30 U.S. companies, including Amazon [AWS] and Apple, by compromising America's technology supply chain, according to extensive interviews with government and corporate sources."

- "Nested on the servers' motherboards, the testers found a tiny microchip, not much bigger than a grain of rice, that wasn't part of the boards' original design... investigators determined that the chips allowed the attackers to create a stealth doorway into any network that included the altered machines."

- Supermicro (supplier to mil/aero customers) implicated

- Findings disputed

Securing the supply chain

1. **Maintain design authority**
2. Manufacture in-house
3. Security of information
4. Counterfeit parts identification/elimination
5. Supplier qualification
6. Repeatability of processes
7. Anti-tamper/information assurance

The response

- Design should ideally not be entrusted to third parties
- Subcontractors must comply with company security procedures
- Subcontracted designs should be verified on receipt
- Assure incoming boards precisely meet original design

Securing the supply chain

1. Maintain design authority
2. **Manufacture in-house**
3. Security of information
4. Counterfeit parts identification/elimination
5. Supplier qualification
6. Repeatability of processes
7. Anti-tamper/information assurance

The response

- Manufacture locally in secure, government-approved in-house facilities
- Total control from goods received to customer shipment
- Provide e.g. optional black dye conformal coating to 'mask' components

Securing the supply chain

1. Manufacture in-house
2. Maintain design authority
3. **Security of information**
4. Counterfeit parts identification/elimination
5. Supplier qualification
6. Repeatability of processes
7. Anti-tamper/information assurance

The response

- Total conformance with ITAR requirements
- All employees trained in export laws
- Robust, secure IT infrastructure meets government guidelines for cybersecurity
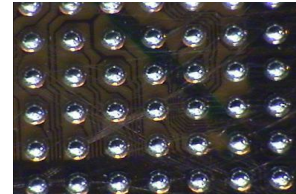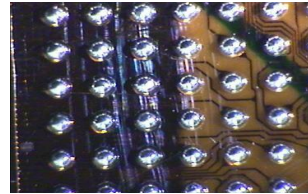 - NIST compliance
- No visitor cameras, portable storage etc.

Securing the supply chain

1. Manufacture in-house
2. Maintain design authority
3. Security of information
4. **Counterfeit parts identification/elimination**
5. Supplier qualification
6. Repeatability of processes
7. Anti-tamper/information assurance

- **50%** of electronics distributors have encountered counterfeit parts

- **58%** of authorised distributors have purchased parts from outside the OCM supply chain to fulfil customer requirements

- **57%** of counterfeit part reports involved obsolete or End Of Life (EOL) parts

Securing the supply chain

1. Manufacture in-house
2. Maintain design authority
3. Security of information
4. **Counterfeit parts identification/elimination**
5. Supplier qualification
6. Repeatability of processes
7. Anti-tamper/information assurance

The response

- All incoming parts examined (down to the screw level)
  - Package permanency markings
  - X-ray difference detection
  - Identification of reclaimed parts
  - Parts marking variances

Securing the supply chain

1. Manufacture in-house
2. Maintain design authority
3. Security of information
4. Counterfeit parts identification/elimination
5. **Supplier qualification**
6. Repeatability of processes
7. Anti-tamper/information assurance

The response

- Purchase only from
  - Original manufacturer
  - Authorized distributor
  - Intensively-vetted distributors
- Routine audits
- Require compliance with standards
- Customer right of approval

Securing the supply chain

1. Manufacture in-house
2. Maintain design authority
3. Security of information
4. Counterfeit parts identification/elimination
5. Supplier qualification
6. **Repeatability of processes**
7. Anti-tamper/information assurance

The response

- Rigorous adherence to quality standards/metrics
- Extensive, repeated training
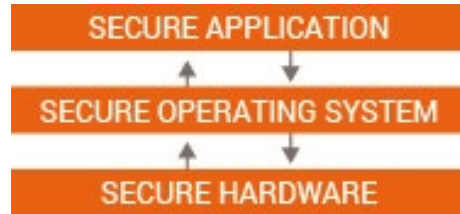
Securing the supply chain

1. Manufacture in-house
2. Maintain design authority
3. Security of information
4. Counterfeit parts identification/elimination
5. Supplier qualification
6. Repeatability of processes
7. **Anti-tamper/information assurance**

The response

Available technologies include:

- Volume protection
- Memory sanitization
- Sensory technologies
- Trusted boot
- Smartfusion2 (Microsemi)
- Intel Trusted Execution Technology

SECURE APPLICATION

SECURE OPERATING SYSTEM

SECURE HARDWARE

Securing the supply chain:
The wider implications.

WE ARE IN THE BUSINESS OF DELIVERING COMPETITIVE ADVANTAGE TO OUR WARFIGHTERS BUT, ABOVE ALL, WE ARE IN THE BUSINESS OF KEEPING THEM SAFE.

Securing the supply chain:
The wider implications.

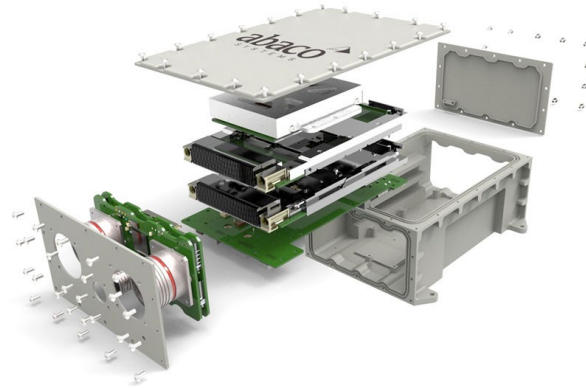1. Robust reliability

2. Long term support

3. Innovation

Securing the supply chain:
The wider implications.

1. Robust reliability

2. Long term support

3. Innovation

The response

- Focus on what 'rugged' really means

- Technology insertion

- Programs to mitigate
  e.g. component obsolescence

- "Innovate to protect"

Securing the supply chain:
The wider implications.

Develop long term trusted partner relationships

Securing the supply chain:
The wider implications.

Develop long term trusted partner relationships.

The response

- Shared goals, shared insights

- Benefits of mutual understanding

- Purely transactional relationships are short-sighted

- Purchase price isn't everything

WE NEVER FORGET THE PEOPLE WE SERVE