

DEFENCE ICT\CYBER PROCUREMENT SUPPLY CHAIN RISK MANAGEMENT FRAMEWORK

SCRMF – An Australian Story

Covering the Who, What, When, How and
Why!!

Chief Information Officer Group ICT Security Branch

- ▶ Lindsay Morgan Assistant Secretary ICT Security (AS ICTS) and Australian Defence Chief Information Security Officer (CISO)
- ▶ John Grady Technical Director ICT Security and soon to take up a Liaison Officer role with US DoD in 2020
- ▶ ICTSB has similar responsibilities to both the Defense Information Systems Agency (DISA) and US CYBERCOM, all be it with a smaller foot print - members and ICT systems
- ▶ AUS Defence is about twice the size of the US Coastguard but a third of size of the Marines

WHO - ARE WE

▶ **ICT\CYBER Procurement SCRM Framework**

- ▶ Reasons for a framework;
 - ▶ Majority of current procurements from untrusted suppliers and supply chains
 - ▶ Majority of current procurements only addressing 'value for money' from an initial procurement perspective
 - ▶ Majority of current procurements not addressing the Capability Life Cycle (CLC); initial procurement, through sustainment and into disposal
 - ▶ Majority of current procurements not being made in accordance with the Financial Delegations given to CIOG for ICT
 - ▶ Leading to the unknown provenance of products and services being used within and to support, sensitive and classified ICT systems
 - ▶ To address the emerging focus on Mission Assurance, Cyber Resilience and Cyberworthiness to ensure operational and mission critical systems will continue to operate within a highly contested, congested and disconnected cyber threat environment

WHAT

Project Scope

Produce a Defence ICT/Cyber Procurement SCRM Framework that:

- Leverages national and international SCRM policy and/or standards;
- Addresses whole of government and five-eyes responsibilities and roles;
- Must cover the capability life cycle.

As necessary and relevant, produce specific ICT/Cyber Procurement SCRM information products

Reality About Supply Chain Risk Management

- There is a lack of guidance, instruction or policy on Supply Chain Risk Management for ICT Procurement in Defence
- WoAG (incl. DTA) does not *currently* look at ICT supply chain risks across the capability lifecycle*
- "DISP provides assurance of the Industry Entity, not their supply chain or goods or services"

Drivers

- Increase in ICT security incidents due to supply chain procurement issues
- Speed of CIOG's ICT delivery is leading to procurement decisions that do not consider security risks
- The Defence procurement officer prioritises cost and timeliness over security
- Defence is not monitoring supply chain security risks (not just ICT – health, logistics, estate, utilities etc.)
- Defence is not compliant with ISM control 1452, DSPF* and PSPF*
- Defence does not adhere to any international standards for supply chain risk management
- Requirement to attain "cyber-worthiness"

ICT/Cyber Supply Chain Threats

Vendor		Products/Service	
Foreign interference and/or influence		Location of factories	Threats
Cyber worthiness		Suppliers	
Security practices		Logistics Operations	Risks
Compliance		Obsolescence	
Reputation			
Financial viability			

Other supply chain risks that impact Defence, but may not be intrinsically linked to ICT/Cyber procurement, include: Environmental (natural, man-made), use of Indigenous suppliers, Health and Safety, Capacity constraints etc.

Stakeholder Requirements

- Implemented across the capability lifecycle
- Direct input from industry through product and vendor information
- Creation of an evaluation capability/team to carry out SCRM processes
- SCRM methodology used across all Defence (and potentially WOAG)
- Considers international SCRM standards
- End database with product and vendor information to improve Defence procurement decisions

Stakeholders (Work Areas Consulted)

12	CIOG
10	CASG
18	Rest of Defence
6	Government
2	Academia
7	Industry

(Estimated) Costs to Defence

\$4-5 MILLION
Approx. total for remediation, investigation and security education as a result of a Defence group's Protected network being compromised.

not just an ICT issue...

Context: In early 2019, a particular type of laptop was procured through an Australian Department store. This laptop was to be used on a Defence Protected Network in order to analyse a specific dataset related to a sensitive project. A few weeks later, this type of laptop was found to have a 'backdoor' flaw, introduced in the manufacturing stage, that could have been used by third-parties to take control of machines.*

Owners	Consequences**
Minister Defence	Reputation
CDF and Secretary	Force preparedness
Army, Navy, Air Force	Business continuity
CIOG	Network remediation and resources
ASD and ACSC	Defence security assessment
DS&S	Contract review
CASG	MILIS data audit
JLC	Audit review for ANAO

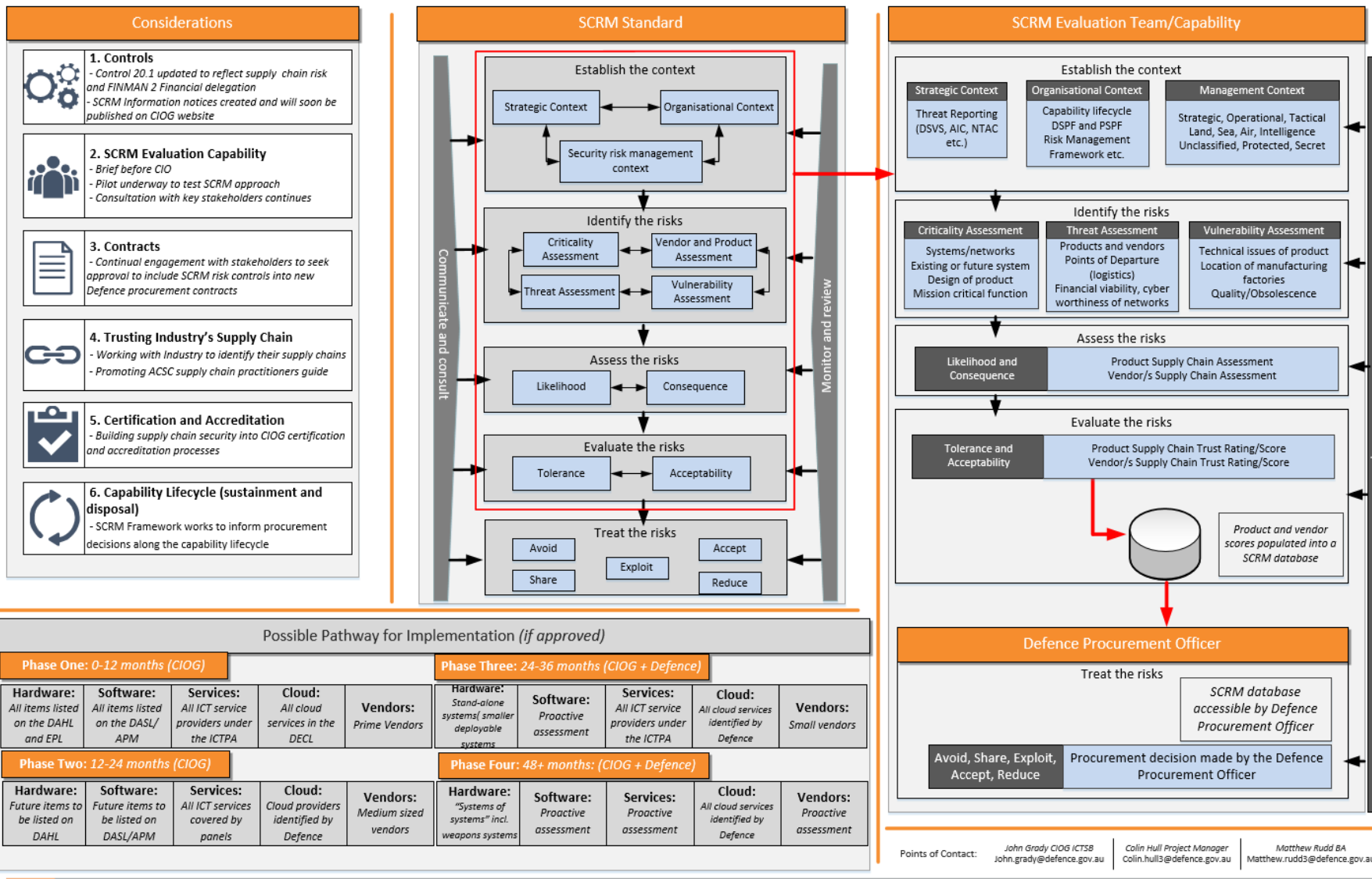
Cyber worthiness

> \$1 BILLION +

52+ Domains
250 known networks
9,000 servers+
113,000 Active users world-wide

ICT/Cyber Supply Chain Security alone does not equal cyber worthiness; it forms part of the overall cyber risk picture.
* - source - bbc.com (3 Apr 2019)
** - only a summary of some consequences that may happen

WHAT



WHAT



Increase in ICT security incidents due to supply chain procurement issues



Timeliness of CIOG's ICT delivery is leading to procurement decisions that do not consider security risks



The Defence procurement officer prioritises cost and timeliness over security



Defence is not actively monitoring supply chain security risks/threats



Defence is not compliant with ISM control 1452, DSPF and PSPF



Defence is not adhering to any international standards for supply chain risk management



Requirement to attain "cyber-worthiness"

WHY

(Estimated) Costs to Defence



> \$1 BILLION +

52+ Domains
250 known networks
9,000 servers+
113,000 Active users world-wide

*not just an ICT
issue...*



Context: In early 2019, a particular type of laptop was procured through an Australian Department store. This laptop was to be used on a Defence Protected Network in order to analyse a specific dataset related to a sensitive project.

A few weeks later, this type of laptop was found to have a 'backdoor' flaw, introduced in the manufacturing stage, that could have been used by third-parties to take control of machines.*



Owners	Consequences**
Minister Defence	Reputation
CDF and Secretary	Force preparedness
Army, Navy, Air Force	Business continuity
CIOG	Network remediation and resources
ASD and ACSC	Defence security assessment
DS&VS	Contract review
CASG	MILIS data audit
JLC	Audit review for ANAO
DFG	

Cyber worthiness











ICT/Cyber Supply Chain Security alone does not equal cyber worthiness; it forms part of the overall cyber risk picture.

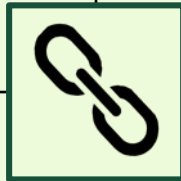
* - source - bbc.com (3 Apr 2019)

** - only a summary of some consequences that may happen

WHY

ICT/Cyber Supply Chain Threats and Risks

Vendor	Products/Service/Cloud
<ul style="list-style-type: none"> Foreign Interference and/or influence Resiliency of networks/systems Security Practices	<ul style="list-style-type: none">Location of factories, transport hubs Suppliers 
<ul style="list-style-type: none"> Compliance (legislation) Reputation Financial viability	<ul style="list-style-type: none">Logistics Operations Obsolescence 



WHAT



Controls

- Update to Defence Security and Policy Framework to include SCRM
- SCRM Awareness Notices created and to be published soon



SCRM Team

- Pilot Underway to test SCRM Methodology
- Consultation with stakeholders continues
- Process mapping to confirm number of staff required, if at all



Contracts

- Engagement with stakeholders has led to SCRM controls be considered for future contractual processes
- Endorsement to include SCRM Framework into Defence's Project Management Manual



Trusting Industry's Supply Chain

- Working with Industry directly, or through Defence Industry bodies to promote supply chain security
- Promoting SCRM practitioner guidance



Certification and Accreditation

- Building supply chain security into Defence's certification and accreditation processes
 - Initially ICT
 - Potentially move into other areas.



Capability Lifecycle

- SCRM Framework works to inform procurement decision throughout the capability lifecycle
- Informs the procurement officer with information about security, warranties and legal obligations.

HOW

- ▶ IOC – commodity ICT SCRM
 - ▶ **FY – 2020/21**
- ▶ IOC+ – ‘systems’ SCRM
 - ▶ **FY 2021/22**
- ▶ FOC – ‘systems of systems’ SCRM
 - ▶ **FY 22/23**

WHEN