MINISTRY OF DEFENCE

BUILDING SECURITY IN

SOFTWARE AND SUPPLY CHAIN ASSURANCE

Fall Forum 2017
Mitre, McLean VA
2017-08-29

Trustworthy Software Foundation

Ian Bryant

Assistant Head of Information Security (Policy)

Standards Development Advisor

[UK/MOD/DAIS/Pol/2017/B/041]

UK OFFICIAL – TLP WHITE

UK Ministry of Defence (MOD)

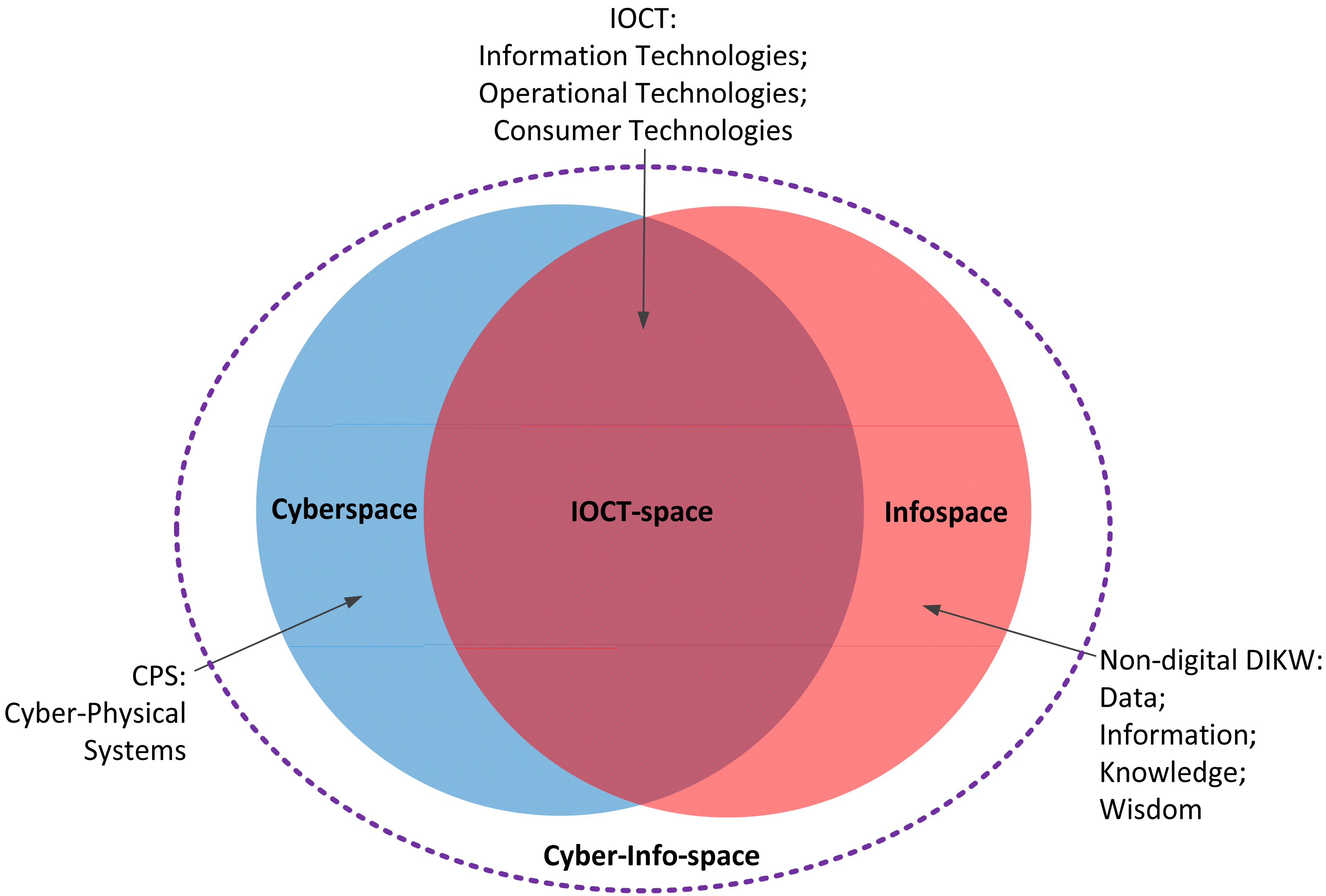
- As a National Defence organisation, MOD is perceived through 3 main “Lenses”:
  - From the view of Government Department

  - From the view of Military Organisation

  - From the view of large acquisition and delivery organisation

- All aspects of operation need to be tailored to best meet (sometimes divergent) requirements of these differing Lenses

Problem Space



IOCT:
Information Technologies;
Operational Technologies;
Consumer Technologies

Cyberspace

IOCT-space

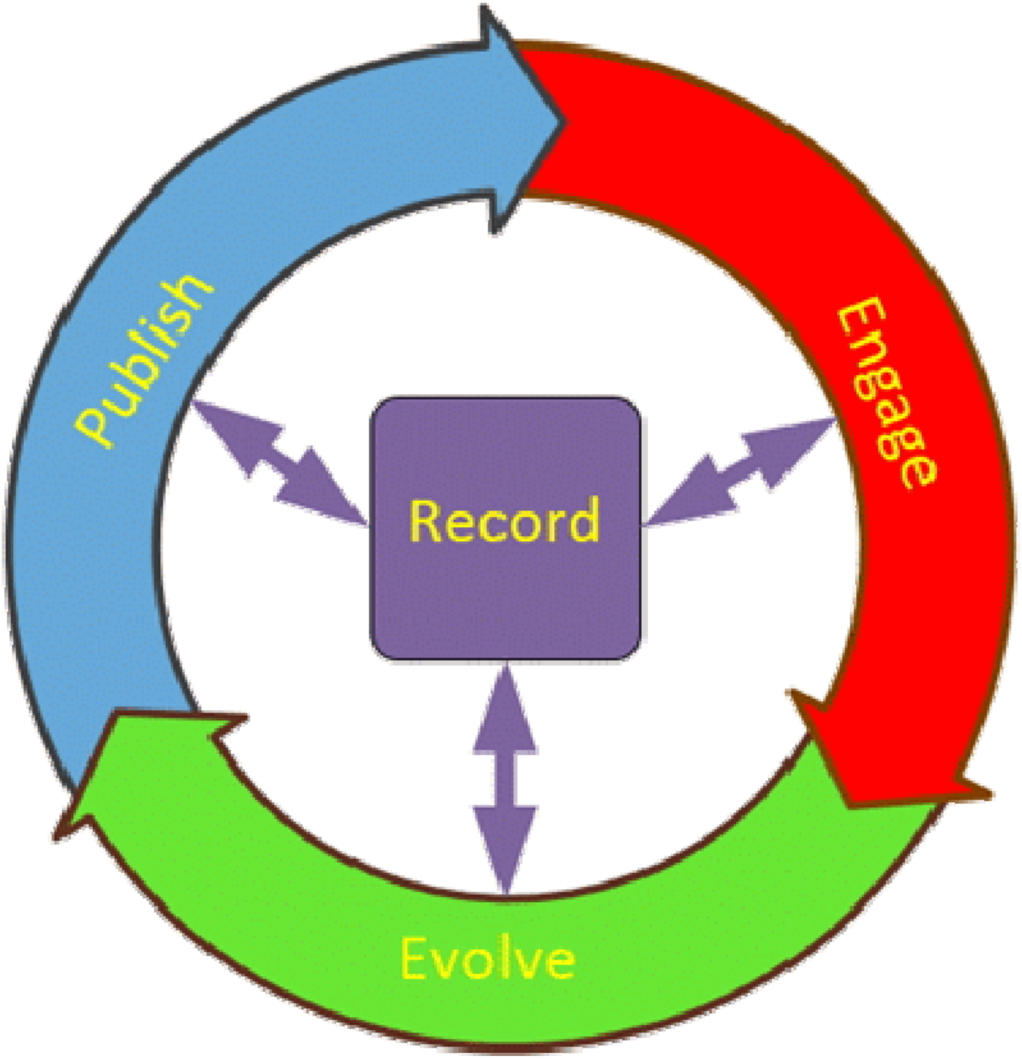
Infospace

CPS:
Cyber-Physical
Systems

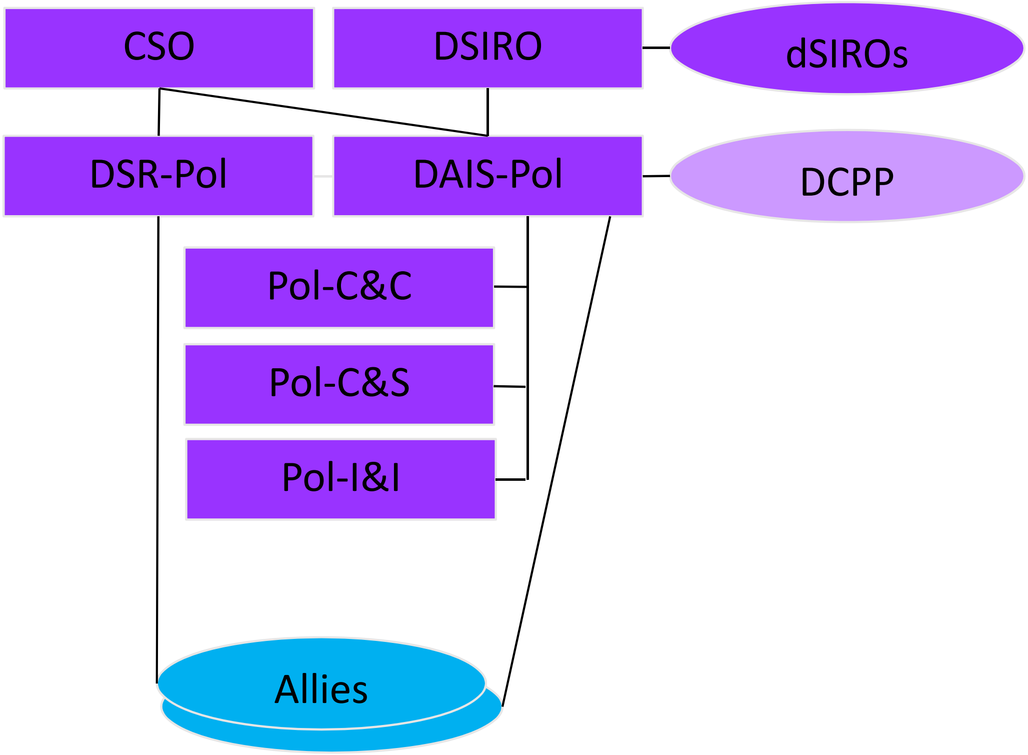
Non-digital DIKW:
Data;
Information;
Knowledge;
Wisdom

Cyber-Info-space

Problem Solving



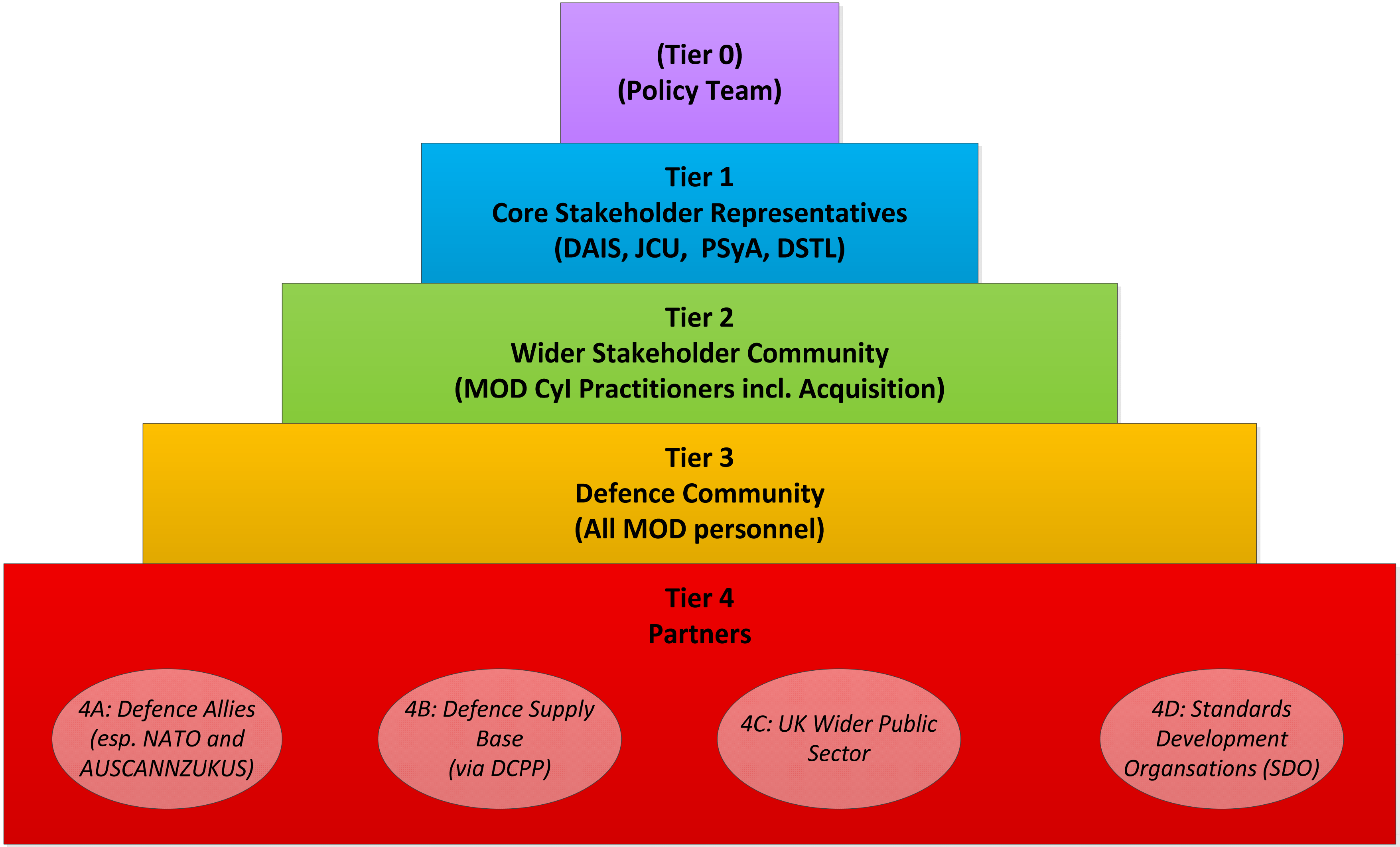
DAIS Policy Branch



CSO = Chief Security Officer
DAIS = Defence Assurance and Information Security
DCPP = Defence Cyber Protection Partnership
dSIRO = delegated Senior Information Risk Owner

DSIRO = Departmental Senior Information Risk Owner
DSR = Defence Security & Resilience
Pol = Policy Branch

Stakeholders



(Tier 0)
(Policy Team)

Tier 1
Core Stakeholder Representatives
(DAIS, JCU, PSyA, DSTL)

Tier 2
Wider Stakeholder Community
(MOD CyI Practitioners incl. Acquisition)

Tier 3
Defence Community
(All MOD personnel)

Tier 4
Partners

4A: Defence Allies (esp. NATO and AUSCANNZUKUS)

4B: Defence Supply Base (via DCPP)

4C: UK Wider Public Sector

4D: Standards Development Organsations (SDO)

Policy Reuse

- Wherever possible seek not to “re-invent the wheel”
- Monitor and/or seek external information / inspiration
- Need for Departmental Wrap† will vary from a simple link to an extensive re-interpretation

Policy

- Sources typically Cabinet Office or NATO

Advice & Guidance

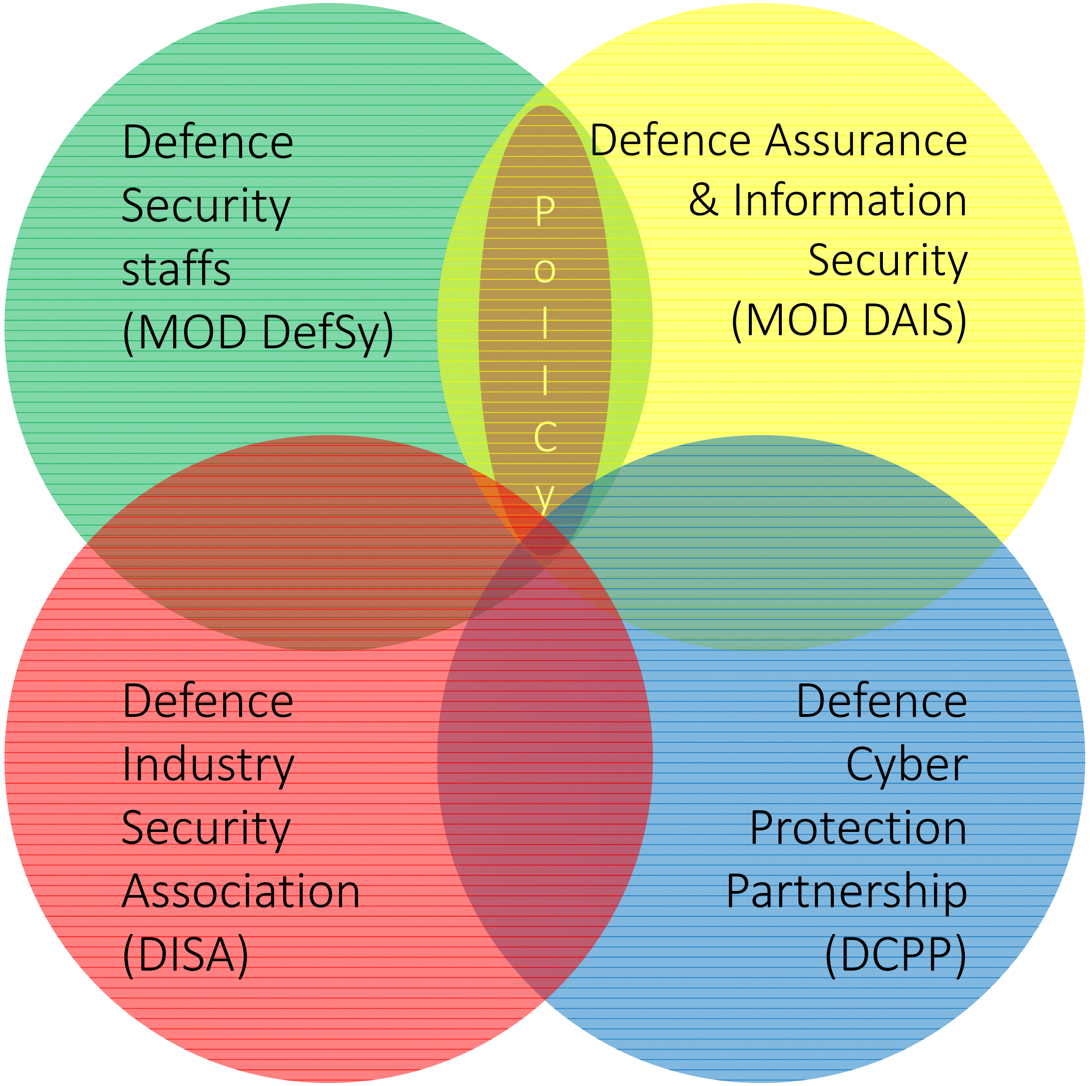
- Sources to include NCSC, GDS, and Allies
- Includes Products and Services

Good Practice

- Wide variety of sources including SDOs and peer relationships

† Cabinet Office, Cyber and Government Security Directorate (CGSD) terminology

Partnering



Defence Security staffs (MOD DefSy)
Defence Assurance & Information Security (MOD DAIS)
Policy
Defence Industry Security Association (DISA)
Defence Cyber Protection Partnership (DCPP)

Context for Outputs

“Act in haste, repent at leisure”

The Old Batchelour

William Congreve (1693)

"Regulations made in haste or without sufficient assessment have a greater potential for adverse effects or unintended consequences"

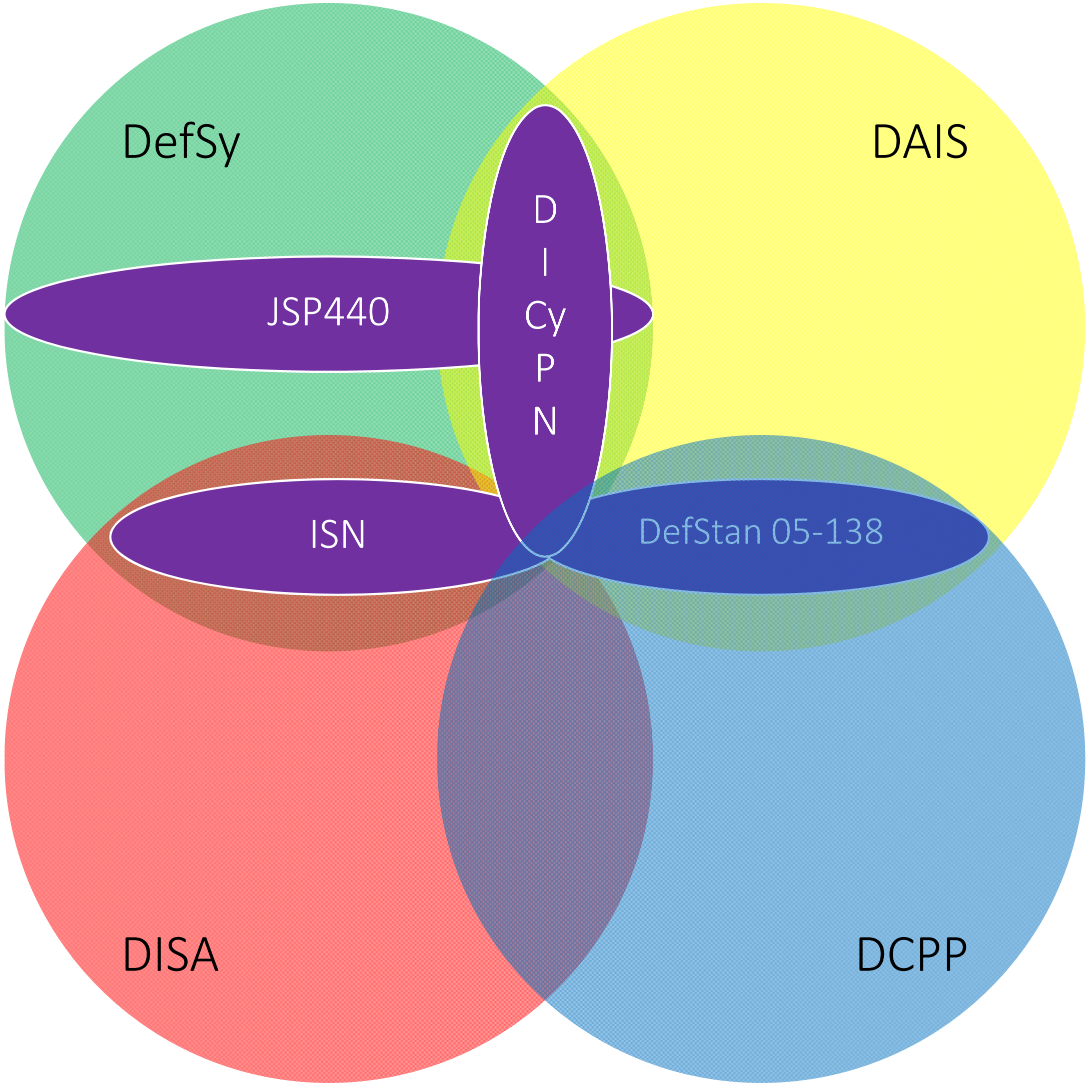
Regulatory Policy in Perspective

OECD (2015)

Output Streams

Stakeholder Engagement Timescale	Nil	Limited	Comprehensive
Needed <1 week from Identification	Advice	✗	✗
Needed <3 months from Identification	✗	Guidance	✗
Can wait >3 months from Identification	✗	✗	Policy

Outputs



- JSP440 – Defence Manual of Security
- ISN – Industrial Security Notices
- DICyPN – Defence Info-Cyber Protection Notices
- DefStan 05-138 – Cyber Security for Defence Suppliers

Market Segmentation

Segment			Treatment	Approach
(No requirement)			TL0	✗
Mass Market / Implicit Need (M/I)			TL1 – Fundamental Practices	→ Commodity
	Mass Market / Explicit Need (M/E)		TL2 – Structured Practices	
		Niche Market / Explicit Need (N/E)	TL3 – Enhanced Practices	Custom
			TL4 – Specialist Practices	

Commodity Marketplace – 2 Views

- Trustworthiness of Organisations in the Supply Chain
  - Defence Cyber Protection Partnership (DCPP)
  - Cyber Security Model (CSM) defined in DefStan 05-138 at Very Low and Low Risk Profiles
  - Linked to Defence Assurance Risk Tool (DART)
- Trustworthiness of Products and Services arising from the Supply Chain
  - Working with BSI and Trustworthy Systems Foundation (TSFdn) to update BS PAS754:2014 (Trustworthy **Software**) to BS10754 series (Trustworthy **Systems**)
  - BS 10754 series will include Baseline Controls (aka TS Essentials)
  - Defence Info-Cyber Protection Advisory Group (DICyPAG) to review and endorse Assured OTS solutions with any necessary Departmental Wrap
  - Challenge area: how to review and endorse Non-Assured OTS solutions

Custom Marketplace – 2 Views

- Trustworthiness of Organisations in the Supply Chain
  - Defence Cyber Protection Partnership (DCPP)
  - Cyber Security Model (CSM) defined in DefStan 05-138 at Medium and High Risk Profiles, supported by Accreditation
  - Linked to Defence Assurance Risk Tool (DART)
- Trustworthiness of Products and Services arising from the Supply Chain
  - Working with BSI and Trustworthy Systems Foundation (TSFdn) to update BS PAS754:2014 (Trustworthy **Software**) to BS10754 series (Trustworthy **Systems**), with Pathway in DART for custom Applications
  - Based on BS 10754 series will include Comprehensive Controls
  - Defence Info-Cyber Protection Advisory Group (DICyPAG) to review and endorse Assured OTS solutions with any necessary Departmental Wrap
  - DICyPAG working with wider Government (JSaRC, NCSC) to identify Gaps

Non-Assured OTS – Possible Approach

- Looking at a formalised approach to monitoring and promulgating the trustworthiness – or lack thereof – of Commodity / Off The Shelf Products and Services
- Proof of Concept S3T (Surveillance Scheme for Solution Trustworthiness)
  - SCA = Supplier Capability Assessment
  - STA = Solution Trustworthiness Assessment
  - Resultant Risk Classes
    - White = Known Good
    - Grey = Not Known Bad
    - Black = Known Bad

Any Questions?

Any Questions ?

Any Questions ?

Any Questions ?

Any Questions ?

Any Questions ?

Contact

Ian Bryant
Assistant Head
(Policy)
Defence Assurance and Information Security

Zone D Floor 0 MOD Main Building
Horseguards Avenue
London SW1A 2HB
United Kingdom

ian.bryant960@mod.uk

tel:+44-20-721-84203

http://www.mod.uk