MINISTRY OF DEFENCE

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

Ian Bryant

Assistant Head of Information Security (Policy)

Trustworthy Software Foundation

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

CPS:
Cyber-Physical Systems

IOCT-space

Infospase

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

Cyber-Info-space
Problem Solving

Publish

Record

Engage

Evolve

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

UK OFFICIAL - TLP WHITE
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

SSCA Fall 2017
[UK/MOD/DAIS/Pol/2017/B/041]
Stakeholders

(Tier 0)
(Policy Team)

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

Tier 2
Wider Stakeholder Community
(MOD Cyl 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
Organisations (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
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

<table>
<thead>
<tr>
<th>Timescale</th>
<th>Stakeholder Engagement</th>
<th>Nil</th>
<th>Limited</th>
<th>Comprehensive</th>
</tr>
</thead>
<tbody>
<tr>
<td>Needed &lt;1 week from Identification</td>
<td></td>
<td>Advice</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>Needed &lt;3 months from Identification</td>
<td>✗</td>
<td>Guidance</td>
<td>✗</td>
<td></td>
</tr>
<tr>
<td>Can wait &gt;3 months from Identification</td>
<td>✗</td>
<td>✗</td>
<td></td>
<td>Policy</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Segment</th>
<th>Treatment</th>
<th>Approach</th>
</tr>
</thead>
<tbody>
<tr>
<td>(No requirement)</td>
<td>TL0</td>
<td></td>
</tr>
<tr>
<td>Mass Market / Implicit Need (M/I)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mass Market / Explicit Need (M/E)</td>
<td>TL1 – Fundamental Practices</td>
<td></td>
</tr>
<tr>
<td>Mass Market / Explicit Need (M/E)</td>
<td>TL2 – Structured Practices</td>
<td>→ Commodity</td>
</tr>
<tr>
<td>Niche Market / Explicit Need (N/E)</td>
<td>TL3 – Enhanced Practices</td>
<td>Custom</td>
</tr>
<tr>
<td>Mass Market / Implicit Need (M/I)</td>
<td>TL4 – Specialist Practices</td>
<td></td>
</tr>
</tbody>
</table>
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

SSCA Fall 2017
[UK/MOD/DAIS/Pol/2017/B/041]
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?
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