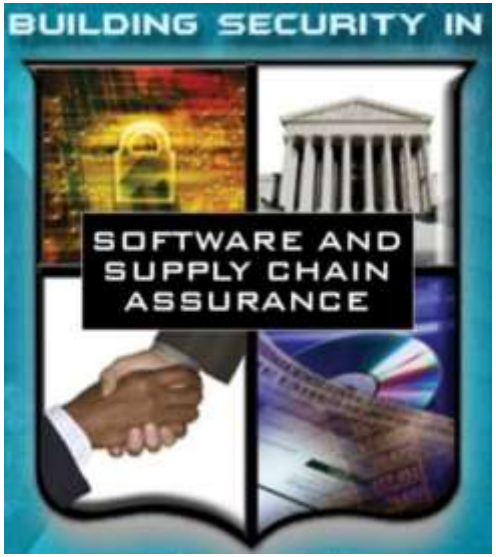


Fall Forum 2017

Mitre, McLean, VA

2017-08-29

Five Eyes Defence CIO Forum (FVEY DCIOF) Supply Chain Assurance working Group (SCAWG)

DCIOF SCAWG – Tasking

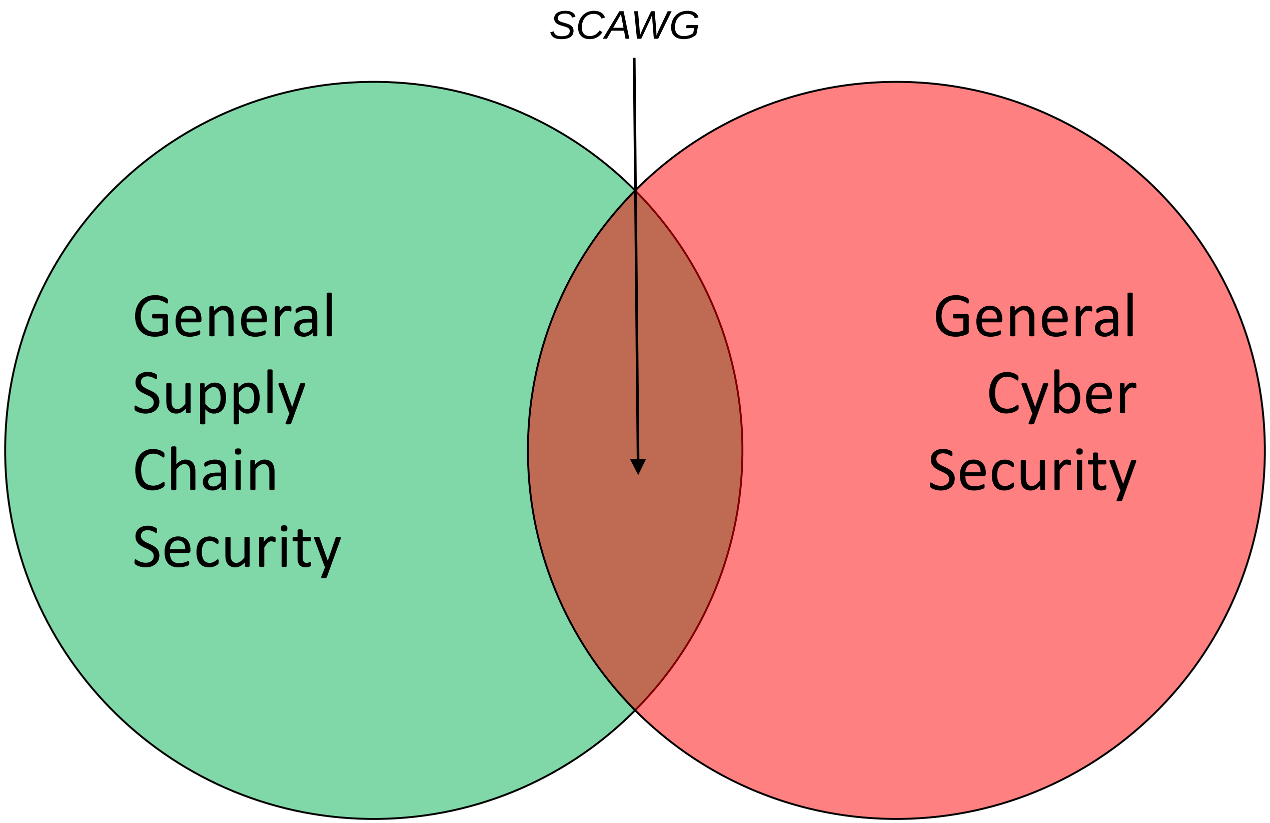
Goal from Principals:

- Achieve a common approach to protection of cyber supply chains across FVEY as a trading block, using common standards

Mission from Principals :

- To either make existing standards compatible, or achieve a common approach

DCIOF SCAWG – Focus



DCIOF SCAWG – Scoping

The initial Scope Review:

- Agreed startup Working Group activity
- Identified what each country has in place

Initial Objectives were agreed to be:

- WP1: Supplier Organisation Assurance Approach
- WP2: Product and Service Assurance Approach
- WP3: Supply Chain Risk Approaches

DCIOF SCAWG – Outline Plan

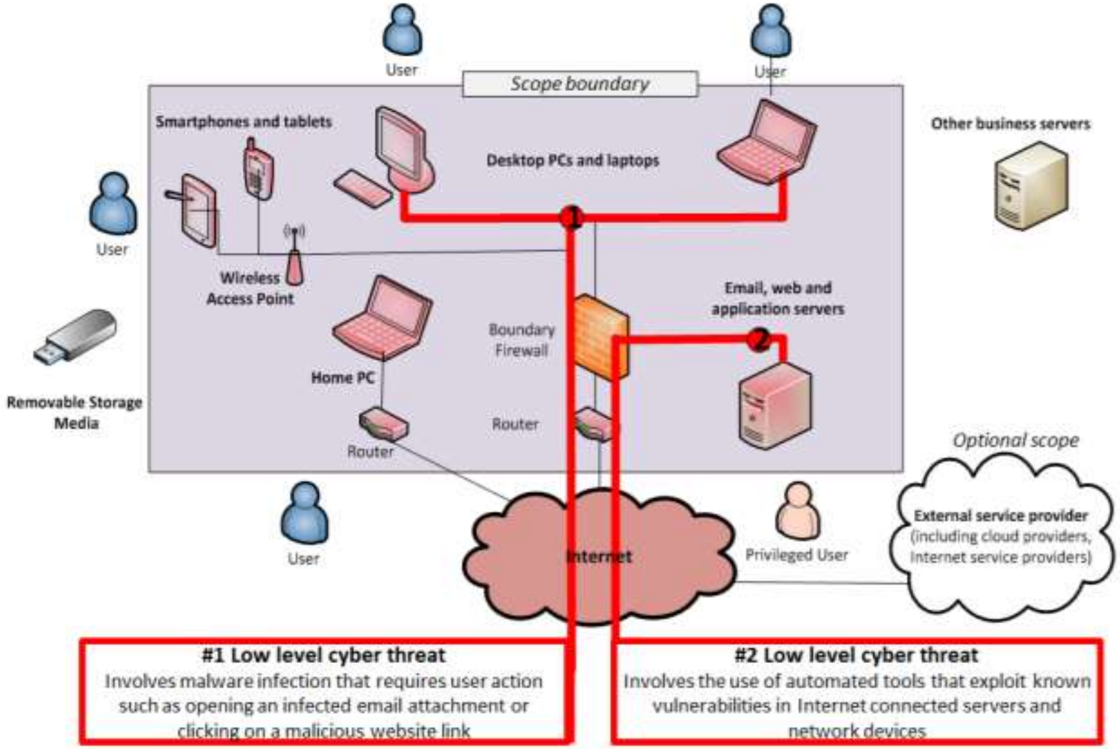
	2Q16	3Q16	4Q16	1Q17	2Q17	3Q17	4Q17	1Q18	2Q18	3Q18	4Q18	1Q19	2Q19	3Q19	4Q19	1Q20
Establishment	▨															
WP1 (Organisations)																
Mutual Discovery		▨	▨													
Evolve Approach				▨	▨	▨										
Promulgate Guidance							▨	▨								
WP2 (Product/Service)																
Mutual Discovery				▨	▨											
Evolve Recognition Approach						▨	▨	▨								
Promulgate Recognition Guidance									▨	▨						
Evolve Surveillance Approach						▨	▨									
Promulgate Surveillance Guidance								▨	▨	▨						
Implement Surveillance Sharing											▨	▨				
WP3 (Risk)																
Mutual Discovery								▨	▨							
Evolve Approach										▨	▨	▨				
Promulgate Guidance													▨	▨		
Implement Sharing															▨	▨
Define Sustainment																▨ ???

DCIOF SCAWG – WP1
Supplier Organisation Assurance Specification

- Objective(s):
  - Develop a mechanism for ‘mutual recognition’ of national specifications
  - Explore convergence to a single standard
- Activity:
  - Coverage analysis completed
  - Existing approaches partially orthogonal
    - UK
    - US
    - SDO e.g. ISO/IEC

DCIOF SCAWG WP1 – Simple Approach

Entry-level of UK's DefStan 05-138 for Supplier Organisation Assurance starts from "Cyber Security Essentials"



#1 Low level cyber threat
Involves malware infection that requires user action such as opening an infected email attachment or clicking on a malicious website link

#2 Low level cyber threat
Involves the use of automated tools that exploit known vulnerabilities in Internet connected servers and network devices

5 Technical Controls

- Boundary firewalls and internet gateways
- Secure configuration
- Access control
- Malware protection
- Patch management

DCIOF SCAWG – WP 1
Supplier Organisation Assurance Specification

Existing approaches / standards, include:

Government

- AUS ISM
- AUS DSPF
- US NIST SP800-161
- US NIST SP800-171
- US DHS FNR CDM
- UK CSE
- UK DefStan 05-138

Public

- ISO/IEC 27000
- ISO/IEC 27001
- ISO/IEC 27002
- ISO/IEC 27010
- ISO/IEC 27036 series

DCIOF SCAWG – WP 1
Supplier Organisation Assurance Specification

TLP AMBER

Five Eyes' (FVEY) Defence CIO Forum (DCIOF)

Supply Chain Assurance Working Group (SCAWG)

WP1: Supplier Organisation

Assurance Interface Specification

(SOIAS)

Version:
0.C DRAFT

Date:
2017-08-28

This document contains DRAFT material, and should not be used as a statement of Policy, nor of Intended Policy, of either the FVEY community, or of any individual member of that community.

Dissemination should be managed in accordance with the TLP Marking applied to the document, as defined in ISO/IEC27010:2015

Page 1 of 18
TLP AMBER

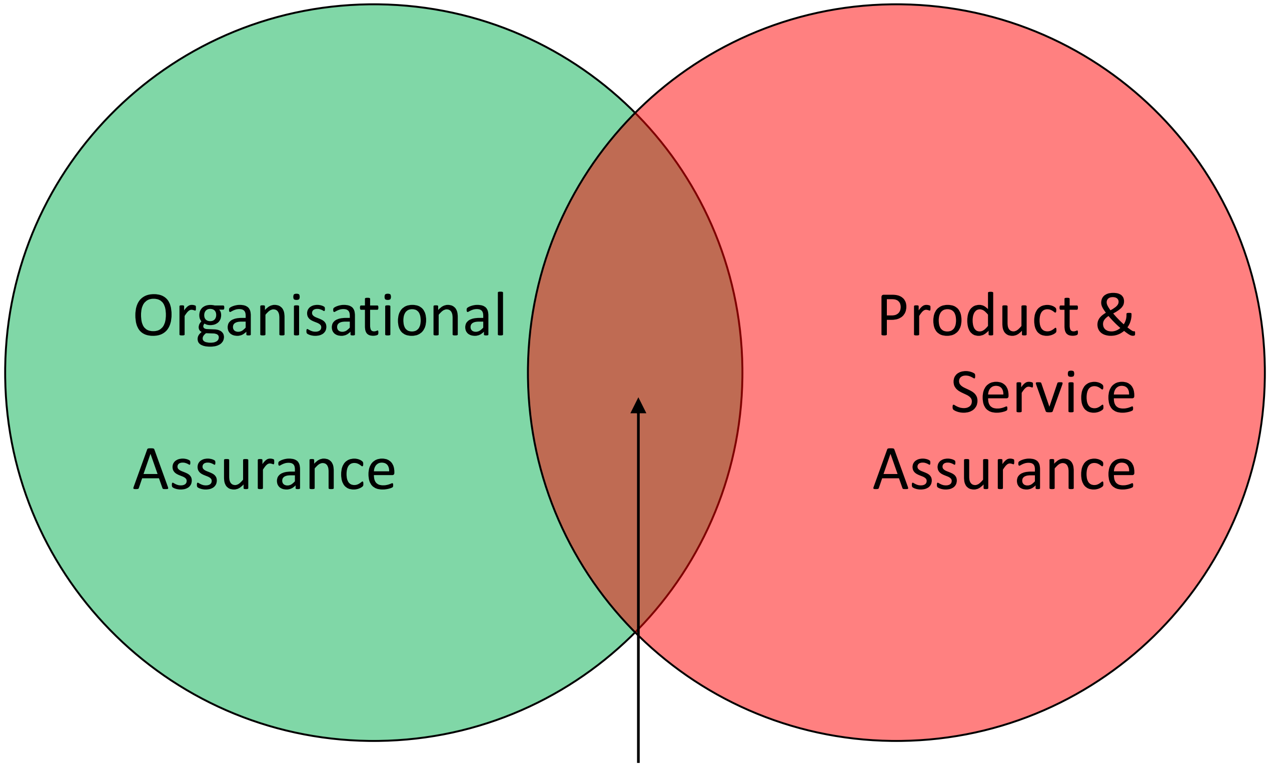
– Interface Specification drafted to allow recognition/reuse

– Planned to scenario test in 4Q2017

DCIOF SCAWG – WP 2
Product and Service Assurance Approach

- Objective(s):
  - Establish common approach to assuring Product and Services from Assured Suppliers (WP1)
  - Scope includes Products (hardware and software) and Services (e.g. cloud)
- Activity:
  - Initial discovery in parallel with Objective 1 Coverage Analysis

DCIOF SCAWG – WP 2
Product and Service Assurance Model



Provides a measure both (a) of confidence in supplier before product/service tested; and (b) of confidence in continued product/service support and evolution

DCIOF SCAWG – WP 2
Product and Service Assurance Approach

- Approach needs to encompass:
  - Whitelisting, of “known good”
  - Greylisting, of “not known bad”
  - Blacklisting, of “known bad”
- Need to link to Post Marketing Surveillance and Flaw Remediation
- Needs to be based on dynamic risk view

DCIOF SCAWG – WP 3
Supply Chain Risk Approaches

- Objective(s):
  - Develop mechanisms, following on from WP1 and WP2, for sharing threat and vulnerability information about (G2G), and with (G2C), supply chains
  - Needs to be based on dynamic risk view
- Activity:
  - (Not commenced yet)
  - (Classification challenges noted)

DCIOF SCAWG – Stakeholders

In addition to Defence, the following parties are (†will be) engaged:

AUS – Government: AGD, ASD, CASG, DIIS

– Industry: t.b.d.†

CAN – Government: CSEC, PWGSC

– Industry: t.b.d. †

NZ – Government: t.b.d. †

– Industry: t.b.d. †

UK – Government: Cabinet Office/CCS, NCSC (ex CESG)

– Industry: DCPP, DISA, UKCeB

US – Government: CNSS, DHS, GSA, NIST

– Industry: SSCA Forum, NDIA, and Others

FVEY DCIOF SCAWG

Australia

New Zealand

FVEY DCIOF SCAWG

Canada

FVEY DCIOF SCAWG

Défense National

National Defence

Canada

Forces Armées Canadiennes

Canadian Armed Forces

CSE

FVEY DCIOF SCAWG

United Kingdom

FVEY DCIOF SCAWG

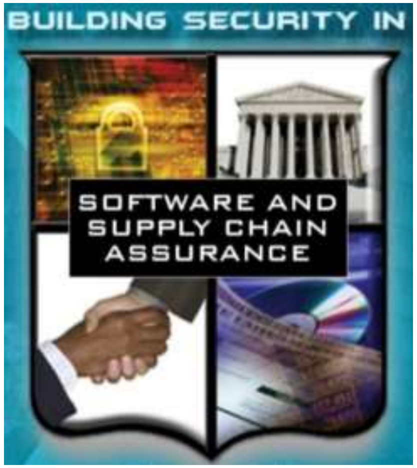
United States of America

FVEY DCIOF SCAWG

United States of America

DEPARTMENT OF DEFENSE

UNITED STATES OF AMERICA



FVEY DCIOF SCAWG

Any Questions?

Five Eyes Defence CIO Forum (FVEY DCIOF)

Supply Chain Assurance Working Group (SCAWG)