ICT SCRM Task Force on SwA Buyer’s Guide for Government Enterprise Customers

Tim Mackey, Synopsys
Sridhar Balasubramanian, NetApp
This work product hasn’t yet published so, Chatham House!!!
Tim’s Bio

Comments are not those of my employer or our official policy

• Joined Synopsys in 2017 as part of the Black Duck acquisition

• Head of Software Supply Chain Risk Strategy
  – Cross portfolio role focused on global regulations
  – Product group advisor on regulatory implementations
  – Strategic resource for client teams in C-suite discussions

• IT Sector Co-chair of DHS CISA ICT SCRM Task Force on SwA

• Worked 13 years at Citrix
  – Virtualization and Cloud lead within Citrix Open Source Business Office
  – Dotted line to Citrix CSO with product security responsibility
Sridhar’s Bio

• Sridhar is currently working as Principal Security Architect within Product Security Group @ NetApp.
• Earlier worked for LSI Storage Systems as Security Architect.
• With over 25 years in software industry, Sridhar is inventor/co-inventor for 15 US Patents and published 9 Conference papers till date.

• Sridhar holds Master's degrees in Physics and Electrical Engineering.
Understanding the ICT SCRM TF SwA WG work product

Status: Currently in NRMC Production for publication

What is it?

Software Assurance Guide for Government Enterprise Consumers: Software Assurance in the Cyber-Supply Chain Risk Management (C-SCRM) Lifecycle

Who was involved in development?

– GSA, NASA, NSA, CISA, and other agencies
– Dozens of IT and Communications sector members as subject matter experts

What is the core objective?

– Develop a vendor questionnaire to aid enterprise procurement and acquisition teams needing to assess the software development, software supply chain, software deployment, and vulnerability policies and practices within software producers
Refresher: What is SwA and why does it matter

Definitions:
1. The level of confidence that software functions as intended and is free of vulnerabilities, either intentionally or unintentionally designed or inserted as part of the software throughout the lifecycle.

Sources:
CNSS 4009-2015 from DoDI 5200.44

2. The planned and systematic set of activities that ensure that software life cycle processes and products conform to requirements, standards, and procedures.

Sources:
CNSS 4009-2015 from NASA-STD 8739.8

The level of confidence that software is free from vulnerabilities, either intentionally designed into the software or accidentally inserted at any time during its life cycle, and that the software functions as intended by the purchaser or user.

Sources:
NISTIR 8074 Vol. 2 under Software Assurance
Sidebar: ICT SCRM Vendor Template provided lessons

- Published April 2021

- **Goal:** Normalize a set of questions regarding an ICT Supplier/Provider implementation and application of industry standards and best practices. This will enable both vendors and customers to communicate in a way that is more consistently understood, predictable, and actionable.

- The buyers guide compliments this template
Where did our authority to create this guide come from?

• “No single set of software assurance practices can address every situation, due to the diversity of computing environments and development and deployment practices”

• The DHS ICT Supply Chain Risk Management (SCRM) Task Force has been a success story, showing that collaboration between IT and Communications sectors and government agencies produces meaningful work products for the whole ICT ecosystem. Continuing this work to include sector-specific implementation guidance of the EO 1402852 software assurance directives is a logical future assignment for the ICT SCRM Task Force.

• The Government could extend partnerships with industry, similar to the model of the DHS Supply Chain Risk Management Task Force, to develop and document more specific SCRM guidelines to better measure, assess, and mitigate downstream risk.
NIST SP 800-53 Rev. 5
Security and Privacy Controls for Information Systems and Organizations

FedRAMP

NIST SP 800-161
C-SCRM Practices

GSA 7700 Attestation Form

NIST SP 800-218
SSDF

Software Acquisition Guide

*Notional - Not to scale
Problem: IT questionnaires have a free-form response bias

Interpretation of questions can lead to incomplete perspectives on conformance

- How do you secure servers hosting the application and the database?
- Is a list of configuration elements required?
- Is alignment certified by 3rd party?
- Do you have ISO 27018 certification for proposed datacenter. If not, how can you demonstrate alignment of your security program to ISO 27018?
- In the event of security incident requires legal action, what forensic procedures are available to support potential legal action subject to the relevant jurisdiction?
- In which jurisdiction and who is the regulator?
- Is this across all systems, processes and policies?
- What is your change management process? Is security review part of the change management process?
Goal: Reduce free-form answers with simple Yes/No options
No compound questions, and any required supporting evidence can come later

Do software updates and upgrades verify the authenticity and ownership of the individual components included in the distribution through cryptographic signatures prior to installing the binary files (e.g., Trusted boot, Verified boot, or Secure boot)?

Does the software supplier have an intrusion detection and monitoring system in place to detect unauthorized activities?

If the supplier provides a SaaS solution, does the software supplier provide a documented SLA for patch application?

Does the software supplier determine secure configurations for software components, and make these available (e.g., as configuration-as-code) so developers can readily use the configurations?
What do suppliers want to answer?

1. 316 detailed process questions
2. 58 control group practices
3. 19 policy focused governance controls
4. All the above
What do procurement teams want to process?

1. 316 detailed process questions
2. 58 control group practices
3. 19 policy focused governance controls
4. All the above
Supporting “Secure by Demand” by focusing on the full SDLC

Even the most securely developed software can be deployed insecurely

Customers should also push their vendors to publicly document the secure by design actions each vendor takes. Collectively, this can create a strong demand signal for security, which can encourage and enable software manufacturers to take steps towards greater security. In other words, just as we seek to create a pervasive secure by design philosophy within software manufacturers, we need to create a “secure by demand” culture with their customers.
We cover a lot of ground, but ease of response was a priority
Using affirmative responses to reduce questionnaire burden
Questions are implicitly linked, so provide credit where it's due

<table>
<thead>
<tr>
<th>Control</th>
<th>Description</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>CONTROL.GOV.01</td>
<td>Does the supplier provide a CISA Secure Software Development Attestation Form without need for a POA&amp;M, signed by the supplier’s designated employee (Chief Executive Officer or designee)?</td>
<td>Yes</td>
</tr>
<tr>
<td>CONTROL.GOV.09</td>
<td>Does the supplier provide a machine-readable SBOM meeting minimum requirements defined by National Telecommunications Information Administration (NTIA) or successor guidance as published by CISA that covers all software components of the product being delivered to the customer organization?</td>
<td>Yes</td>
</tr>
<tr>
<td>CONTROL.GOV.18</td>
<td>Do software supplier’s procurement, outsourcing, and contractual agreements, such as Service Level Agreements (SLAs), stipulate that their sub-suppliers and/or service providers follow secure SDLC practices, scan for undocumented, unused, or obsolete functions, and notify the software supplier of identified vulnerabilities or security incidents?</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Only 3 questions answered addresses 29 controls and 167 tasks.

i.e. Credit is given for 29 control questions and 167 task questions

<table>
<thead>
<tr>
<th>Response Status</th>
<th>Yes</th>
<th>No</th>
<th>Skipped</th>
<th>Unanswered</th>
</tr>
</thead>
<tbody>
<tr>
<td>Governance</td>
<td>3</td>
<td>0</td>
<td>N/A</td>
<td>16</td>
</tr>
<tr>
<td>Controls</td>
<td>0</td>
<td>0</td>
<td>29</td>
<td>29</td>
</tr>
<tr>
<td>Tasks</td>
<td>0</td>
<td>0</td>
<td>167</td>
<td>149</td>
</tr>
</tbody>
</table>
Let’s do a quick demo ....
Providing attestation evidence via SBOM – SPDX 2.3 format

externalRefs:
- comment: “GSA 7700 Attestation Form"
  referenceCategory: "OTHER"
- comment: “FedRAMP Authorization"
  referenceCategory: "OTHER"
- comment: “Supplier SBOM"
  referenceCategory: "OTHER"
MITRE System of Trust (SoT)

- The goal of SoT is to offer a comprehensive and consistent methodology that can be tailored to meet industry and company needs to address supply chain security issues, leading to better traceability, reliability, and security of supply chains.

- The SwA Acquisition Guide utilizes similar set of controls as in SoT framework to evaluate software publishers as part of procurement decisions.
Mapping: MITRE SoT to SwA Acquisition Guide

Example: Training risks

<table>
<thead>
<tr>
<th>(RC-76) Supplier Organizational Security Risks</th>
</tr>
</thead>
<tbody>
<tr>
<td>(RC-403) Technical Operations Risks</td>
</tr>
<tr>
<td>(RC-441) Cyber Threat Intelligence Risks</td>
</tr>
<tr>
<td>(RC-16) Security Training Deficiencies</td>
</tr>
<tr>
<td>(RC-346) Security Capabilities and Operations Risks</td>
</tr>
<tr>
<td>(RC-434) Cyber Threat Activity Risks</td>
</tr>
<tr>
<td>(RC-400) Security Governance and Compliance Risks</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CONTROL.GOV.14</th>
</tr>
</thead>
<tbody>
<tr>
<td>Does software supplier provide role-based SDLC-related training and have qualified personnel and/or automated processes that contribute to all parts of the SDLC, including secure architecture, development, testing and threat modeling?</td>
</tr>
<tr>
<td>If 'Yes,' then the following Software Development CONTROL questions and associated TASK questions can be skipped: DEV.04, DEV.05, DEV.18</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CONTROL.DEV.05</th>
</tr>
</thead>
<tbody>
<tr>
<td>Does the software supplier provide periodically updated role based, SDLC related training for all personnel with responsibilities that contribute to secure architecture, development, testing and threat modeling?</td>
</tr>
<tr>
<td>TASK.DEV.05.01</td>
</tr>
<tr>
<td>TASK.DEV.05.02</td>
</tr>
<tr>
<td>TASK.DEV.05.03</td>
</tr>
<tr>
<td>TASK.DEV.05.04</td>
</tr>
<tr>
<td>TASK.DEV.05.05</td>
</tr>
<tr>
<td>TASK.DEV.05.06</td>
</tr>
</tbody>
</table>
Mapping: MITRE SoT to SwA Acquisition Guide (Contd..)

Example: SDLC risks

<table>
<thead>
<tr>
<th>(RC346) Security Capabilities and Operations Risks</th>
</tr>
</thead>
<tbody>
<tr>
<td>(RC-346) Technical Operations Risks</td>
</tr>
<tr>
<td>(RC-403) Cyber Threat Intelligence Risks</td>
</tr>
<tr>
<td>(RC-16) Security Training Deficiencies</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>GOVERNANCE Control</th>
<th>Supply Chain</th>
<th>Software Development</th>
<th>Software Deployment</th>
<th>Vulnerability Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>GOV.01 Secure Software Development - Attestation Form</td>
<td>SC.04, SC.07, SC.08</td>
<td>DEV.03, DEV.07, DEV.08, DEV.09, DEV.10, DEV.11, DEV.12, DEV.14, DEV.20, DEV.21, DEV.22, DEV.23, DEV.26, DEV.27, DEV.28, DEV.30</td>
<td>DEP.07, DEP.09, DEP.11</td>
<td>VULN.01, VULN.04, VULN.07</td>
</tr>
<tr>
<td>GOV.02 Data Provenance</td>
<td>SC.01, SC.04, SC.08</td>
<td>DEV.03, DEV.12, DEV.16, DEV.30</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GOV.03 Vulnerability Mitigation</td>
<td>SC.07</td>
<td>DEV.09, DEV.24</td>
<td>DEP.03, DEP.04, DEP.09, DEP.12</td>
<td>VULN.02, VULN.03, VULN.04, VULN.05, VULN.06, VULN.08</td>
</tr>
<tr>
<td>GOV.04 KEY Testing</td>
<td></td>
<td>DEV.21, DEV.22, DEV.27, DEV.28, DEV.30</td>
<td>VULN.02, VULN.05, VULN.06</td>
<td></td>
</tr>
<tr>
<td>GOV.05 Vulnerability Mitigation</td>
<td></td>
<td>DEV.30</td>
<td></td>
<td>VULN.01, VULN.03, VULN.07, VULN.08</td>
</tr>
<tr>
<td>GOV.06 Secure by Default</td>
<td></td>
<td>DEV.29</td>
<td>DEP.01, DEP.07, DEP.11</td>
<td></td>
</tr>
<tr>
<td>GOV.07 Zero-Trust and Secure by Design</td>
<td></td>
<td>DEV.01, DEV.03, DEV.07, DEV.08, DEV.09, DEV.11, DEV.12, DEV.10, DEV.18, DEV.20, DEV.23, DEV.26</td>
<td>DEP.10</td>
<td></td>
</tr>
</tbody>
</table>
Questions?
Thank You