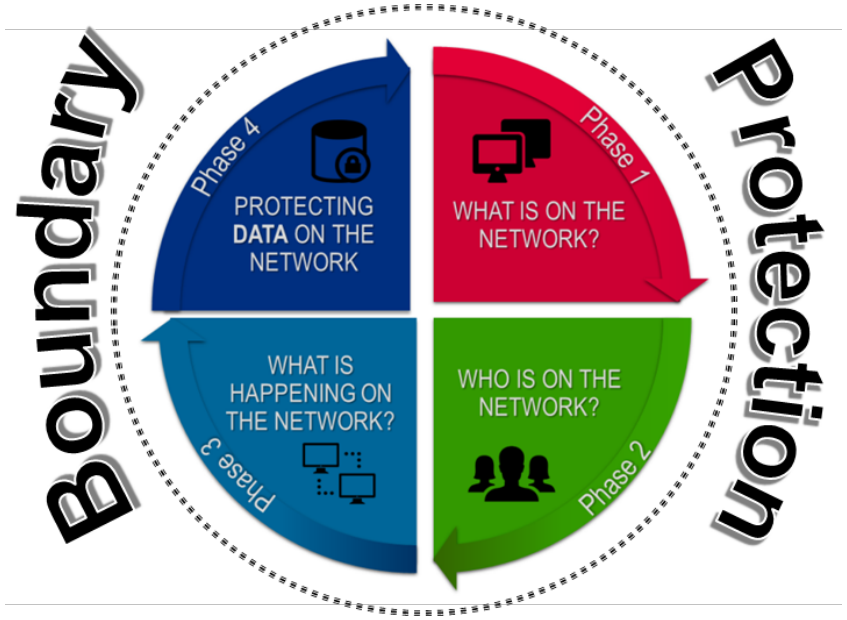
SCRM for CDM Products

CDM Tools Approved Products List (APL)
Supply Chain Risk Management Plan Overview

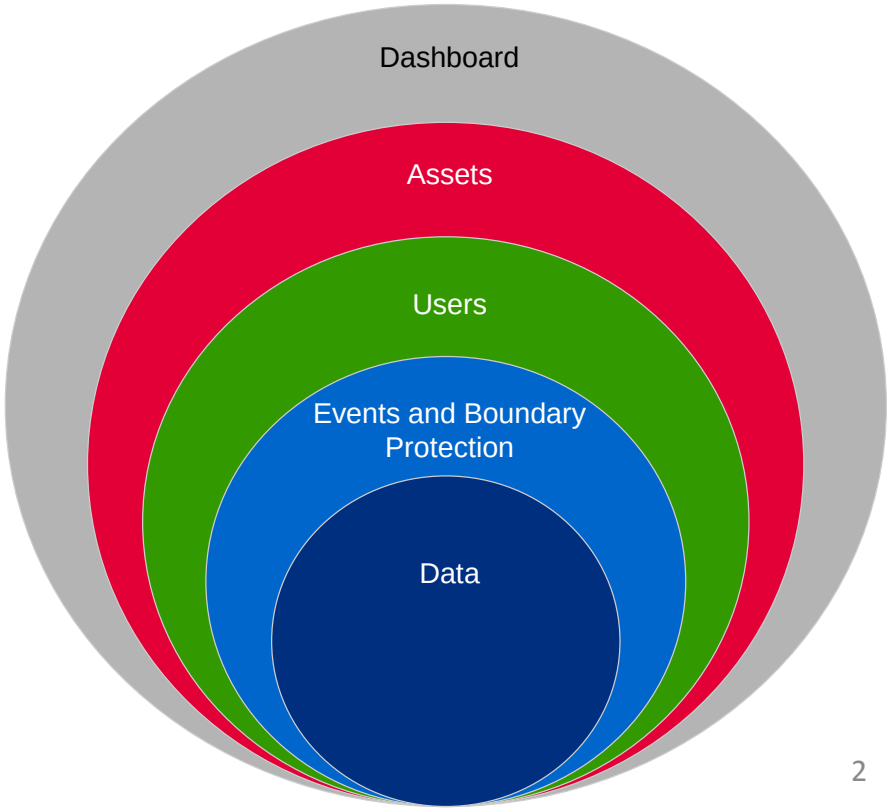
Briefing for CISQ Cyber Resilience Summit

October 19, 2017

Continuous Diagnostics and Mitigation (CDM) Overview



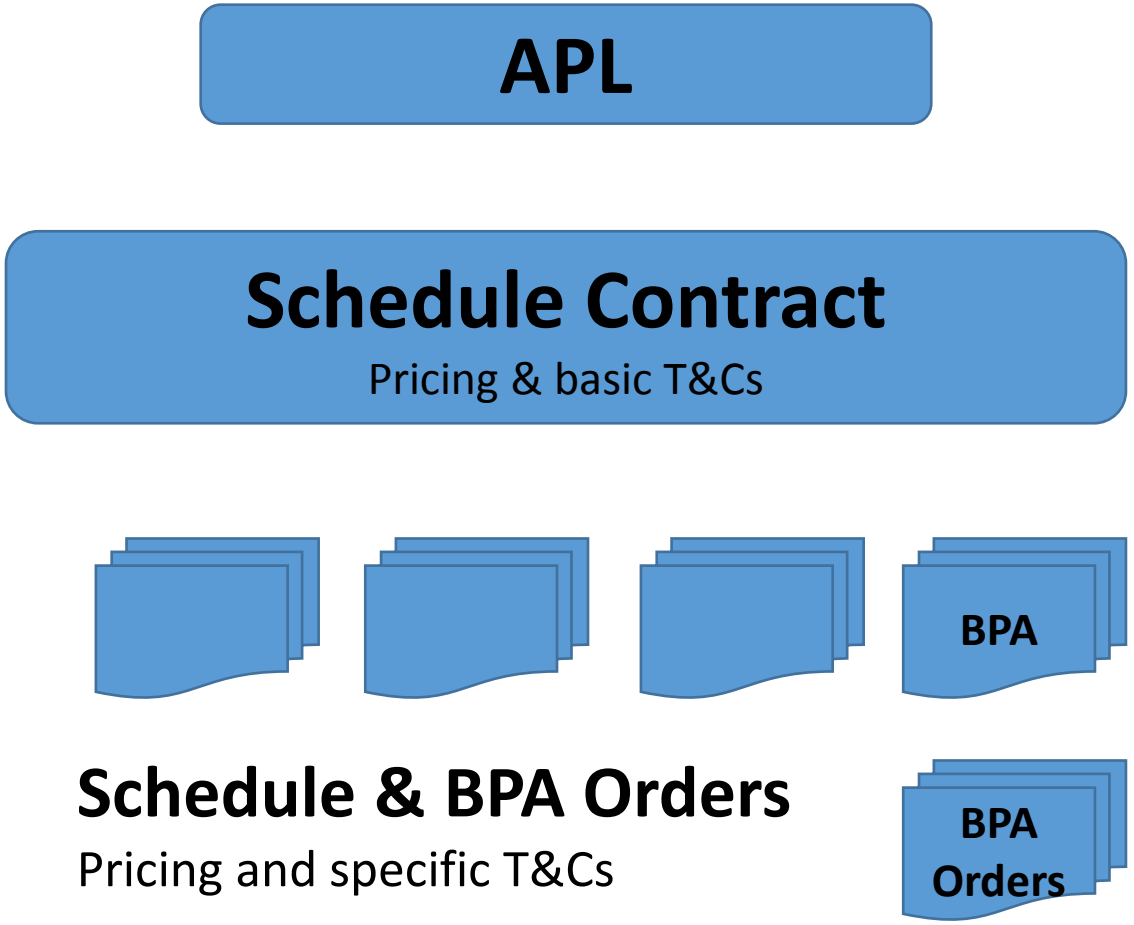
- Provides hardware, software, and services to federal civilian agencies (.gov) so they can better manage and secure their information systems.
- Deploying in phases across 70 agencies including 23 Chief Financial Officer (CFO) Act agencies.



- CDM data feeds report to an agency-level dashboard for display and action. Aggregation from agency dashboards feed into a federal-level dashboard to assist in security oversight and reporting.
- Dashboards will also provide risk scoring to network operators so they can prioritize the most critical issues.

GSA IT Schedule 70 Overview

- Delivers federal, state, and local customer agencies the tools and expertise needed to shorten procurement cycles, ensure compliance, and obtain the best value for innovative technology products, services, and solutions.
- More than 7.5 million products and services from over 4,600 vendors.
- GSA awards and administers Schedule contracts containing basic pricing, terms and conditions.
- Authorized ordering activities place orders under Schedule contracts for specific requirements.



CDM Tools “Special Item Number” (SIN)

- DHS and GSA collaborated to create the new CDM Tools "Special Item Number" (SIN) for GSA's Schedule 70 IT program.
- Includes COTS IT products that meet one or more of the CDM program technical requirements and are listed on the CDM Approved Products List (APL).
  - Note: Approved product is not automatically added to the SIN. Product must be on APL before Offeror requests GSA add it to SIN via contract award or modification.
- Division of labor is that DHS manages the APL and GSA manages the Schedule 70 contracts.
- More information about the CDM Tools SIN is found here: https://gsa.gov/portal/content/167606.

APL Product Submission and Evaluation Process

- To get a product listed on the CDM APL, offerors submit a proposal which, among other things, includes the information required for DHS to assess the product against the APL qualification criteria, found here: https://gsa.gov/portal/getMediaData?mediaId=167742
- DHS notifies GSA and the Offeror of APL evaluation result.
- After a product is qualified and Offeror submits formal request, GSA may add it to the CDM SIN.
- Once the product is listed on the CDM SIN or the APL, the APL SCRM Plans are made available to authorized ordering activities upon request.

APL SCRM Plan

- One of the APL qualification criteria is the completed SCRM Plan.
- SCRM Plan Instructions found here: https://gsa.gov/portal/getMediaData?mediaId=167734.
- Product Assurance and Supplier Management Questionnaires found here: https://gsa.gov/portal/getMediaData?mediaId=167746.

CDM APL SCRM Plan - Product Assurance Questionairre			
Product Manufacturer:			
Product Family:			
		Yes/No	**Notes/Comments**
Does the manufacturer use a SDLC that incorporates software assurance and is measured for effectiveness and/or maturity (e.g., Build Security In Maturity Model (BSIMM), MITRE Assurance)?			
If yes: Is there documentation on the following:			
	SDLC used by the manufacturer to include the overall process of incorporating both system functionality and especially security into all the SDLC phases, from requirement to development to deployment ?		
	The manufacturer's system/software development methods?		
	The manufacturer's security engineering methods?		
	The manufacturer's quality control processes to include test and evaluation?		
	The manufacturer's activities to minimize the number of vulnerabilities/weaknesses and incorporate appropriate update mechanisms for mitigation?		
Does manufacturer conduct analysis of all compiled code to identify all third-party commercial and open source components and all known vulnerabilities/weaknesses found in the National Vulnerability Database (nvd.nist.gov/)?			
	If yes, are the results documented?		
Does manufacturer conduct analysis of how the product behaves during operation and whether such behavior introduces potential security vulnerabilities that could negatively impact confidentiality, integrity, and availability?			
	If yes, are the results documented?		
Does manufacturer conduct scans of software to determine if any known malware exists in the software and a risk assessment on mitigation controls or value of risk?			
	If yes, are the results documented?		
Does manufacturer conduct Security Test and Evaluation (ST&E) on the product offered?			
If yes, does Security Test and Evaluation (ST&E) determine:			
	Whether the required configurations for operations adhere to recommended best practices such as identified within government guidelines such as United States Government Configuration Baseline (USGCB) and associated Defense Information Systems Agency Security Technical Implementation Guides (STIGs)?		
	That all ports, interfaces, and services are documented and that there exists no undocumented port, interface, or service?		
	That all ports, interfaces, and services that require authentication meet the requirements of NIST SP 800-63 or other equivalent applicable standard?		
	That all software and hardware weaknesses that are identified in the product that are listed as critical or high in the National Vulnerability Database and/or otherwise negatively impact confidentiality, availability, and integrity of the supplier's product have been effectively mitigated?		
Will manufacturer provide, for all deliveries of software, firmware, or any product that contains an executable component, a comprehensive and confidentially supplied list of each third party commercial or open-source executable component used in the software, firmware, or product, including the component's version number?			
Do the proposed products have the capability to perform remote system maintenance, software upgrades, troubleshooting, and diagnostics?			
If yes, does the remote mechanism:			
	Utilize strong authentication for access to products?		
	Assure the download packages are unaltered, malware-free and from an uncompromised supplier		
Will the manufacturer make any or all of the documentation identified above plus additional information about its product assurance practices available if requested by an Agency or ordering activity?			

CDM APL SCRM Plan - Supplier Management Questionairre			
Product Manufacturer:			
Product Family:			
		Yes/No	**Notes/Comments**
Are manufacturer's supply chain risk management processes identified, established, assessed, managed, and agreed to by organizational stakeholders?			
	If yes, is there documentation about the manufacturer's supply chain risk management processes?		
Does manufacturer identify, prioritize and assess suppliers and partners of critical information systems, components and services using a supply chain risk assessment process?			
	If yes, is there documentation about how the manufacturer's assesses and prioritizes suppliers?		
Are manufacturer's suppliers and partners required to implement appropriate measures designed to meet the objectives of the APL Supply Chain Risk Management Plan (i.e., do measures include product assurance and supplier management equivalent to or substantively similar to the requirements of the APL SCRM Plan)?			
	If yes, if requested by an Agency or ordering activity, will the Offeror provide additional information about what measures are required by the Offeror or the manufacturer?		
Are manufacturer's suppliers and partners monitored to confirm that they have satisfied their obligations as required?			
	If yes, is there documentation about how manufacturer monitors suppliers' compliance?		
Does manufacturer conduct reviews of audits, summaries of test results, or other equivalent evaluations of suppliers/providers?			
	If yes, is there documentation on how evaluations are reviewed?		
Does manufacturer conduct response and recovery planning and testing with critical suppliers/providers?			
	If yes, is there documentation about how the manufacturer tests the suppliers?		
Will the manufacturer make make any or all of the documentation identified above plus additional information about its supplier management practices available if requested by an Agency or ordering activity?			

APL SCRM Plan Assessment

- The content of the SCRM Plans is not assessed by DHS during the APL qualification process.
- The SCRM Plan is only reviewed by DHS to ensure completeness - i.e., the offeror answered all of the questions.
- For now, no differentiation between SCRM Plans is provided by DHS.
- It is expected that ordering activities will use the SCRM Plans to differentiate between offerors for specific orders from the CDM SIN.
  - E.g., Buyer uses the SCRM Plan information (and/or gets more information from offerors) as part of market research and solution architecture and design.

Notes on Content of CDM SCRM Plans

- The questionnaires highlight specific areas of supply chain risk engineers and program managers should pay attention to when building a CDM solution.
- DHS does not provide a prioritization of those risk areas.
- SCRM Plan is a starting point for better informed decisions.
- Provenance/Chain of custody and requirement for OEM/Authorized purchasing are not addressed in the SCRM Plan because they are both strict requirements for all proposed products.