Continuous Diagnostics and Mitigation (CDM) Tools Special Item Number (SIN)

presented by
Shon Lyublanovits

Table of Contents

CDM Tools/CMaaS BPA

15 Tool Functional Areas

- Hardware Asset Management
- Software Asset Management
- Configuration Management
- Vulnerability Management
- Manage Network Access Controls
- Manage Trust-in-People Granted Access
- Manage Security Related Behavior
- Manage Credentials and Authentication
- Manage Account Access
- Prepare for Contingencies and Incidents
- Respond to Contingencies and Incidents
- Requirements, Policy, and Planning
- Design and Build-in Quality
- Manage Audit Information
- Manage Operation Security

11 Service Task Areas

- Provide Order Project Management Support
- CDM Order Planning
- Support CDM Dashboards
- Provide Specified Tools and Sensors
- Configure and Customize Tools and Sensors
- Maintain Data on Desired State for CDM Tools and Sensors
- Operate CDM Tools and Sensors
- Integrate and Maintain Interoperability between CDM Tools and Legacy Applications and Data
- Operate Data Feeds to and from Installed Dashboards
- Training and Consulting in CDM Governance for D/As and other Requesting Organizations
- Support Independent Verification & Validation and System Certification

Period of Performance:	August 12, 2013 - August 11, 2018
Administered by:	GSA/FAS/AAS/FEDSIM Program Office
BPA Awardees:	16
Current Sales:	$700 million
Order Types:	Labor Hour Firm Fixed Price Cost Reimbursable
CDM Program Phases:	CDM Products (Tools) CDM Services CDM Integration

CDM Tools SIN

The CDM Tools SIN is being created to replace the current CDM Tools/CMaaS BPA.

CDM Tools SIN Considerations:

- Create a SIN to replace the tools portion of the current BPA
- Scope: 5 Subcategories with 15 Tool Functional Areas (TFAs) and Emerging Tools and Technology

Once a CDM tool is approved in the APL validation process, it will be offered under one or more of the following Tool Functional Area (TFA) categories:

Manage "What is on the network"		Manage "Who is on the network"		Manage "How is the network protected"	
TFA 1	Hardware Asset Mgmt	TFA 6	Manage Trust in People Granted Access	TFA 10	Prepare for Contingencies and Incidents
TFA 2	Software Asset Mgmt	TFA 7	Manage Security Related Behavior	TFA 11	Respond to Contingencies and Incidents
TFA 3	Configuration Mgmt	TFA 8	Manage Credential and Authentication	TFA 12	Design and Build in Requirements, Policy and Planning
TFA 4	Vulnerability Mgmt	TFA 9	Manage Account/Access/ Manage Privileges	TFA 13	Design and Build in Quality
Manage "What is happening on the network"		Emerging Tools and Technology		TFA 14	Manage Audit Information
TFA 5	Manage Network Access Controls	TFA x	Includes CDM tools and technology not in any other category	TFA 15	Manage Operation Security

CDM Tools SIN RFI

The purpose of the CDM Tools RFI was to gain:

- Industry perspective on the establishment of the CDM Tools SIN
- Understanding of any administrative or technical hurdles that may exist when deploying CDM Tools onto agency networks and gain a better understanding of:
  - Barriers to entering the market
  - Pros/cons of the Approved Products List (APL) validation process
  - Issues with contract structures
  - Partnership agreements or needs
  - Incorporation of innovative technologies
  - Difficulties with the SIN modification process

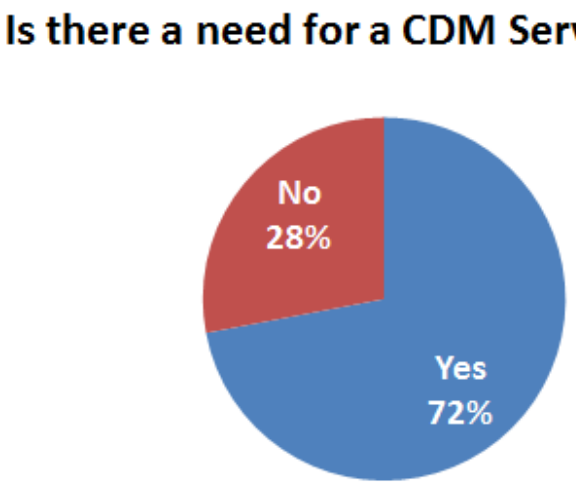
Released: March 22, 2017
Closed: April 5, 2017

The RFI requested feedback from Industry on the proposed SIN for the 15 CDM Tool Functional Areas (TFA). There were a total of 52 respondents to this RFI. Below is a breakdown of the respondents:

	Number	Percentage
Large Businesses	29	56%
Small Businesses	23	44%
On IT Schedule 70	42	81%
Not on IT Schedule 70	10	19%
5+ Years in Business	44	85%

Industry respondents highlight the following technology categories for potential enrollment in Category 5 “Emerging Tools and Technology:”

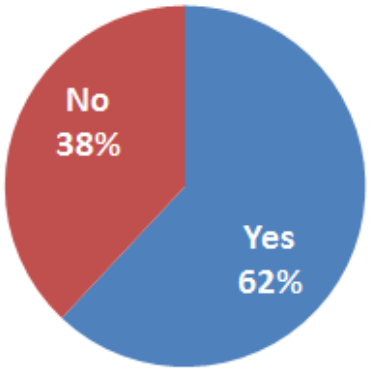
- Network Architecture Framework
- Mobile/Internet of Things Device Security Monitoring
- Micro-segmentation Security
- Unified Security Intelligence



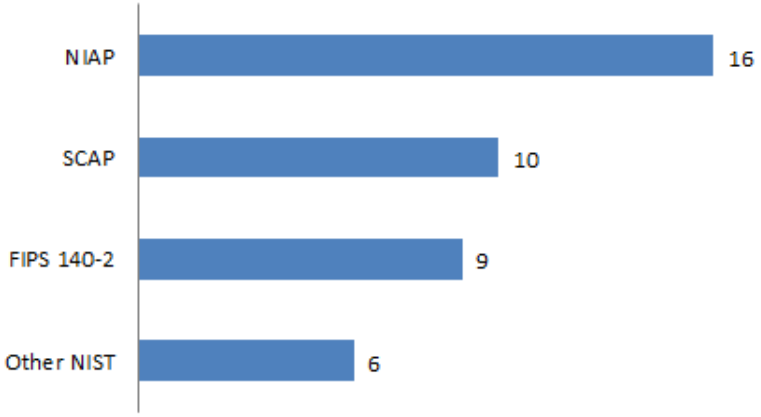
Key Advantage:
CDM services are essential to ensure proper functioning of tools.

Key Disadvantage:
A separate CDM Services SIN might present needless complication to the CDM acquisition process.

Have your tools been evaluated?

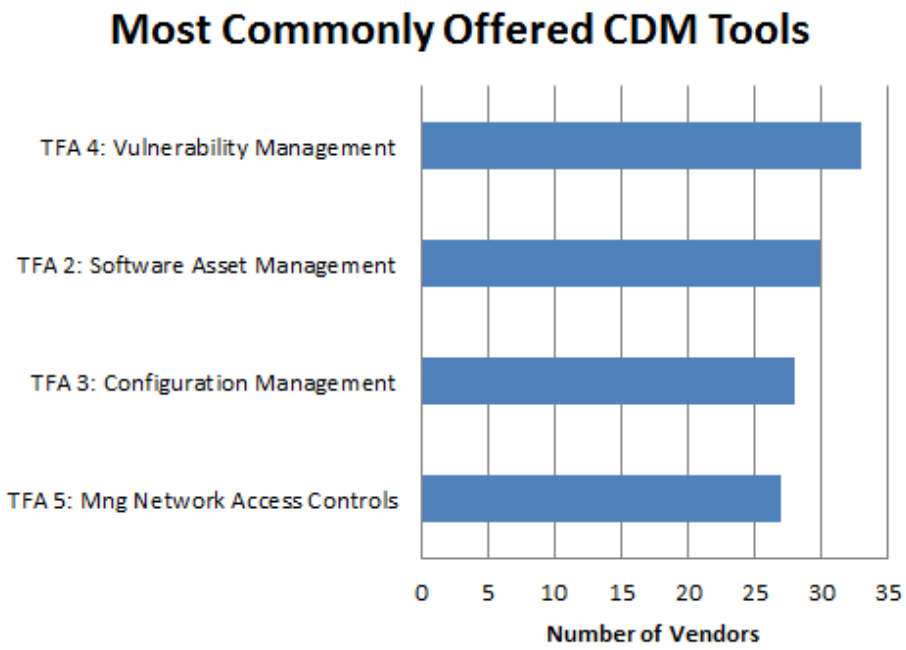


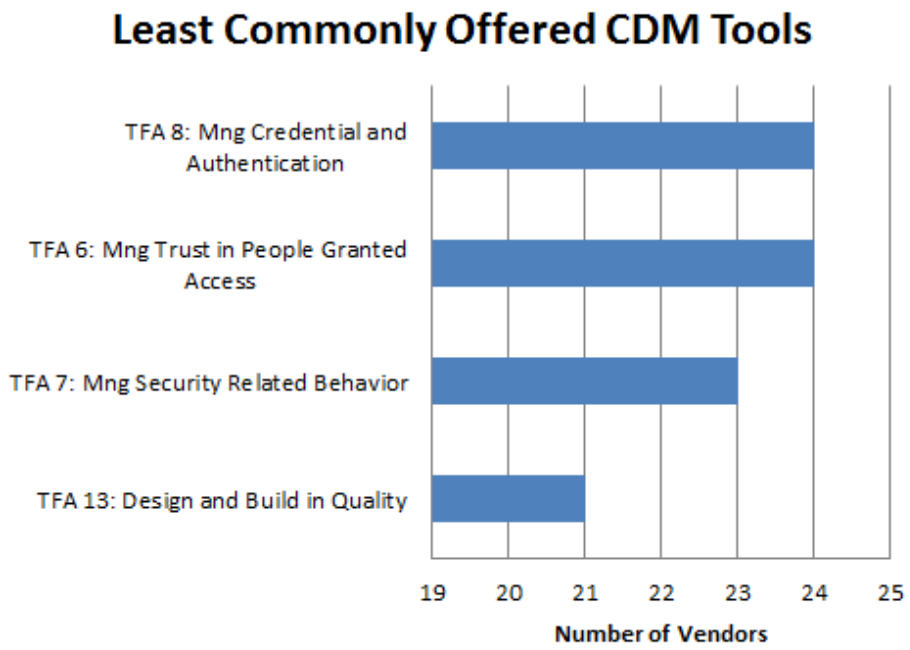
Most Common Evaluation Bodies



Respondents report holding a variety of agency-specific product certifications such as the US Army NETCOM's Certificate of Networthiness.

Percentage of vendors currently on CDM/Continuous Monitoring as a Service (CMaaS) Blanket Purchase Agreement (BPA): 52%





Each TFA is offered by roughly 40-60% of the respondents.

There is a general consensus that the current proposed SIN description is appropriately formulated and accurately covers the government's intent in streamlining how CDM tools are sold.

The main concerns respondents have with the proposed CDM SIN description are:

- Excessive focus on tools designed to protect the network rather than the assets that reside on it
- Overly broad descriptions of the subcategories and TFAs
- Ill-defined nature of Category 5 (Emerging Technology), which will increase difficulty in addressing any product requirements

Respondents made additional comments in this RFI:

- The SIN should include analytics engines/tools to identify data patterns which could be used to manage residual risk and/or shore up gaps in an agency's security posture
- Make the application process transparent
- GSA/DHS should be concerned about the ability of agencies to purchase CDM tools from an APL without regard to the procurement of attendant CMaaS services
- The modification and update process still needs to be more streamlined and responsive

Conclusion

Conclusion

With the establishment of the CDM Tools SIN, GSA and DHS both seek to establish periods of performance beyond the expiration of the current CDM Tools/CMaaS BPA.

By working in close collaboration with other agencies and our Industry partners, we strive for a seamless transition from the BPA to the SIN, one that will improve technology offerings for our customers, while providing an agreeable marketplace for the businesses that supply them.