Continuous Diagnostics and Mitigation (CDM)

CDM SIN Industry Day

April 17, 2017

Topics

- CDM Program Overview
  - CDM Successes
- Transition to CDM SIN
  - BPA and Successes
  - Transition
  - APL and Process
- CDM Requirements
- Questions

CDM Program Overview

Kevin Cox, CDM Program Manager

DHS Team – CDM SIN

DHS Point of Contact	Role
Kevin Cox	CDM Program Manager
Jim Quinn	CDM Lead Systems Engineer
Niki Lane	CDM Acquisition and Requirements Management Branch Chief
Cristen Cole	CDM Acquisition and Requirements Management Deputy Branch Chief

CDM Program Overview

- Focused on securing the entire civilian .gov network by providing hardware, software, and services to Federal civilian agencies (.gov) so they can strengthen their ability to better manage and protect their information systems.
- Deploying in Phases across 70 civilian agencies including 23 Chief Financial Officer (CFO) Act agencies.

- CDM scans 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 reporting to network operators so they are better able to respond to the known, or most severe, issues first.

CDM Successes

- 75 agencies have signed MOAs with CDM PMO
  - 23 CFO Act Agencies participate in CDM
  - 52 smaller Agencies participate or will participate in current/future CDM Shared Services
- Key successes to date:
  - During asset discovery, developed a stronger understanding of the asset counts in the agencies to secure against the threat.
  - Deploying tools/sensors to all CFO Act Agencies.
  - Increased standardization of security tools and began deployment of agency dashboards to automate reporting and keep the data current.
  - Achieved increased savings (~$600M) through the consolidation of tool purchases reflecting up to a 70% savings compared to IT Schedule 70.
  - Shared services platform will be ready in Q3 FY17 for non-CFO Act Agencies

Future of CDM Acquisitions

- Two part acquisition approach to continue to provide tools and services to protect the .gov networks
  - Tools (Hardware and Software)
    - Maintain the current product catalog from the CDM Blanket Purchase Agreements via the CDM SIN
  - Services

Transition to CDM SIN

Cristen Cole, CDM Acquisition and Requirements Management Deputy Branch Chief

CDM Blanket Purchase Agreement (BPA)

- August 2013: DHS, in partnership with GSA, established a government-wide BPA for Federal, State, Local and Tribal governments to procure information security continuous monitoring (ISCM) tools and services
  - Expires in August 2018

- 17 BPA Holders
  - Approx. 80 unique CTAs
  - Approx. 170K products

BPA Successes

- Orders
  - 39 orders issued against BPA - $650,217,752.26
    - 14 DO/DB by Federal agencies - $31,489,106.20
      - DOI, DOL, SEC, USITC, DHS components
- Products
  - 169,667 SKUs
  - ~150 unique product manufacturers
  - ~570 unique product families
- Tools Deployed
  - ~3,000 product purchases supporting 37 agencies

Transition to CDM SIN

- As directed in OMB M-14-03:
  - Provides vehicle to **continue** to provide a consistent, government-wide set of information security continuous monitoring (ISCM) tools
  - Allows for Federal, State, Local, Regional and Tribal to **continue** to access ISCM tools
  - Leverages the buying power of the federal government to minimize costs associated with procurements

Purpose of SIN

- Establish a government-wide contracting solution to continue to provide a consistent set of information security continuous monitoring (ISCM) tools

Total # of SKUS	169,667
Total # of manufacturers	~150
Total # of Product Families	~570

  - DHS has qualified approximately 170K products against CDM detailed tool requirements
    - SIN will allow these previously approved products to be transitioned to SIN without having to be re-evaluated.
  - DHS will conduct evaluations of new products for potential inclusion on the CDM SIN

Purpose of SIN cont.

- Enhance the ability of offerors to bring new and innovative solutions to the CDM Program
  - Emerging Tools and Technology
    - New sub-category allows products to be proposed for the CDM SIN without pre-existing CDM detailed tool requirements
    - Utilizing the GSA Making It Easier – Startup Springboard initiative
      - Reduction of the 2 year corp experience requirement to allow innovative companies with new technologies the ability to obtain a schedule contract and offer their products/solutions
    - Utilizing the GSA FASt Lane for shorter schedule modification timelines, and new offers

Purpose of SIN cont.

- Improve Government access to the best available technology and improve the flexibility of the CDM Program
  - Utilizing the GSA IT Schedule 70 program to manage such a large product catalog that was previously managed by the BPA Process
  - Direct access to CDM products via GSA IT Schedule 70 and the SIN
    - Increases the ease of buying by customers
  - Direct access for offerors
    - Reseller vs Integrator

DHS Approved Product List (APL)

- Existing CDM Product Catalog – all products that have been evaluated and approved against the BPA
  - Products will continue to be added through DHS evaluation process
  - Products cannot be added to CDM SIN unless product is approved on APL
- The authoritative approved product catalog for products that meet CDM requirements
- APL will be categorized by:
  - Product Manufacturer
  - Product Family
  - Mapping to Subcategory
- Managed outside of GSA by DHS Acquisition and Requirements Branch of the CDM PMO

DHS APL Evaluation Process

- Submission
  - Offeror submits evaluation package to DHS for review
    - Product Evaluation Form
    - Supporting Documentation
- DHS conducts conformance on package
  - If conformance is failed, DHS notifies vendor and provides areas of non-conformance for resubmission
- DHS conducts technical evaluation of package against tool capability requirements
  - If acceptable, DHS notifies vendor that product has been approved and will be added to CDM APL. A courtesy copy to GSA FAStLane with GSA instructions to requires modification to be provided
  - If not acceptable, DHS notifies vendor and identifies areas of non-acceptance
- DHS will update the APL and post to website

DHS APL Form

- Elements of Form
  - Company Information
  - Product Information
    - Product Manufacturer, Product Family, # of products within family
  - Supporting Documentation:
    - VPAT, EULA, SCRM Plan
  - Mandatory requirements:
    - CDM Common requirements
    - Tool Capability Requirements, as applicable
    - Justification

DHS APL Benefits

- Technical Evaluation independent of Price Evaluation
- Direct access to CDM Products
  - Increases ease of buying
- Direct access for offeror
  - Reseller vs Integrator
- Product catalog managed by the GSA Schedules Program (GSA Advantage)
- Leverages government buying power for increased discounts and cost savings

CDM Requirements

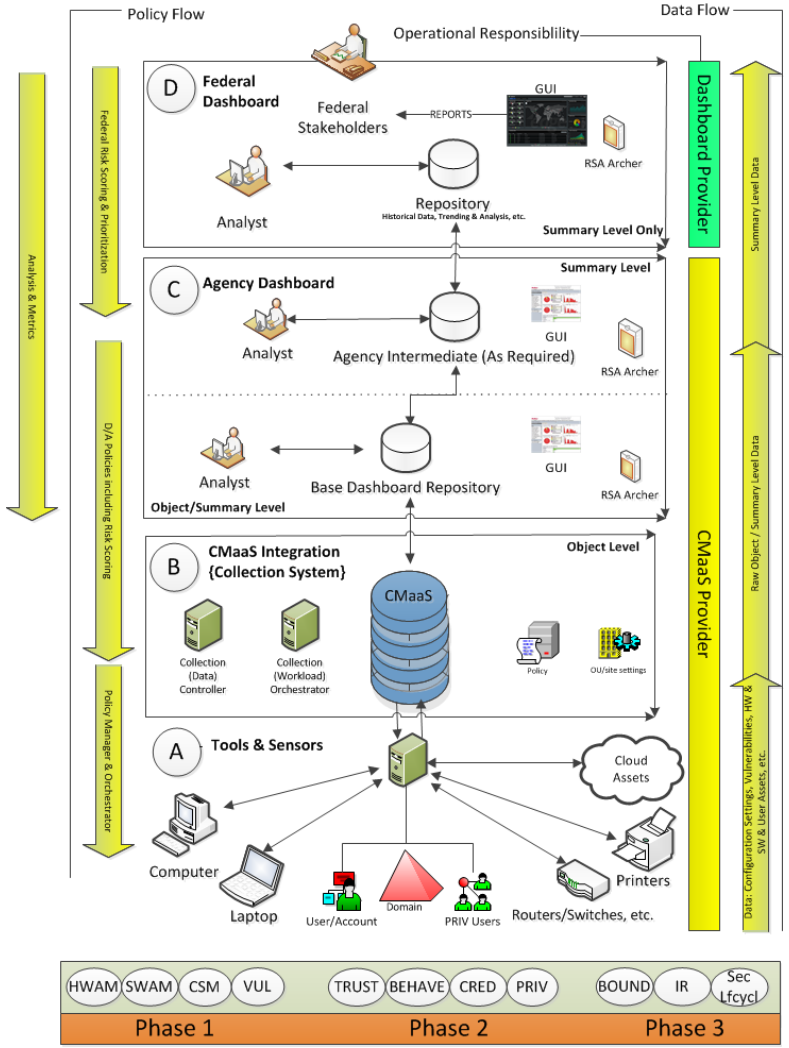
Jim Quinn, CDM Lead System Engineer

Transition to SIN

CDM/CMaaS Blanket Purchase Agreement (BPA) TFAs	Phase	CDM/CMaaS BPA Attachment N	SIN Sub-Category
• TFA 1 – Hardware Asset Management • TFA 2 – Software Asset Management • TFA 3 – Configuration Settings Management • TFA 4 – Vulnerability Management	Phase 1	Phase 1 Attachment N Requirements	Manage “What is on the network?”
• TFA 6 – Manage Trust in People Granted Access • TFA 7 – Manage Security-Related Behavior • TFA 9 – Manage Credential and Authentication • TFA 9 – Manage Account/Access/Manage Privileges	Phase 2	Phase 2 Attachment N-2 Requirements	Manage “Who is on the network?”
• TFA 5 – Manage Network Access Controls	Phase 3	Phase 3 Attachment N-BOUND Requirements	Manage “How is the network protected?”
• TFA 10 – Prepare for Contingencies and Incidents • TFA 11 – Respond to Contingencies and Incidents • Ongoing Assessment	Phase 3	Phase 3 Attachment N-3-Manage Events Requirements	Manage “What is happening on the network?” for MNGEVT
• TFA 12 – Design and Build in Requirements Policy and Planning • TFA 13 – Design and Build in Quality • Supply Chain Risk Management	Phase 3	Phase 3 Attachment N-3-Design and Build in Security Requirements	Manage “What is happening on the network?” for DBS
• TFA 14 – Manage Audit Information • TFA 15 – Manage Operation Security • Ongoing Authorization	Phase 3	Phase 3 Attachment N-3-Operate, Monitor and Improve Requirements	Manage “What is happening on the network?” for OMI
	Phase 4 and beyond	N/A	Emerging Tools and Technology

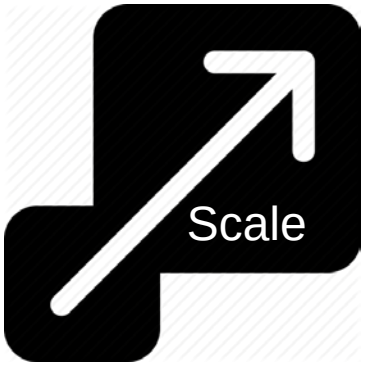
CDM Requirements: COTS Based Architecture

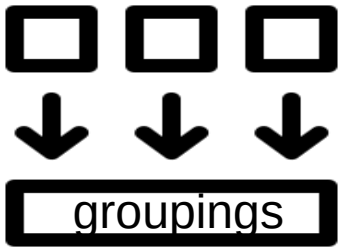
- Architectural boundaries-
  - Zone A: Tools and Sensors
  - Zone B: CMaaS Integration
  - Zone C: Agency Dashboard
  - Zone D: Federal Dashboard
- Dashboard operates as a Standardization Driver
  - Dashboard Provider focused on Federal Level
  - CMaaS Provider focus for Agency Level

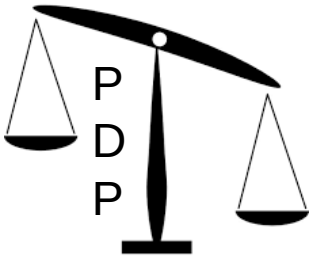


CDM Requirements - "Common"

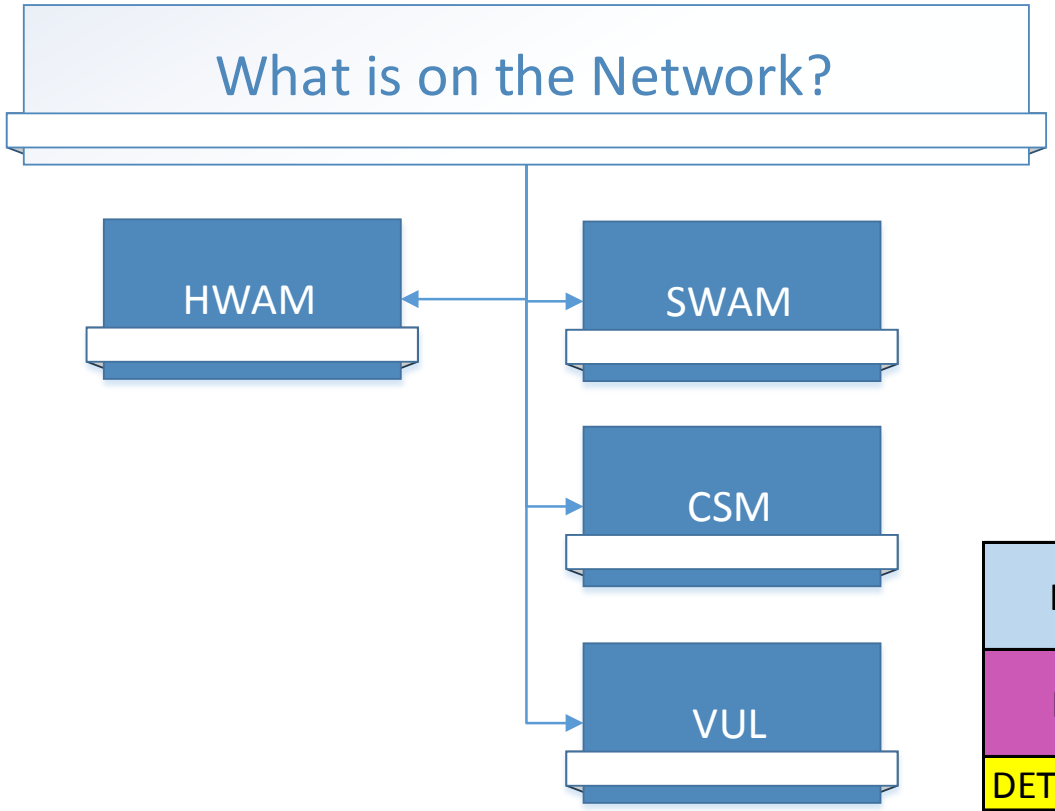
Across all CDM Phases, there are the common requirements





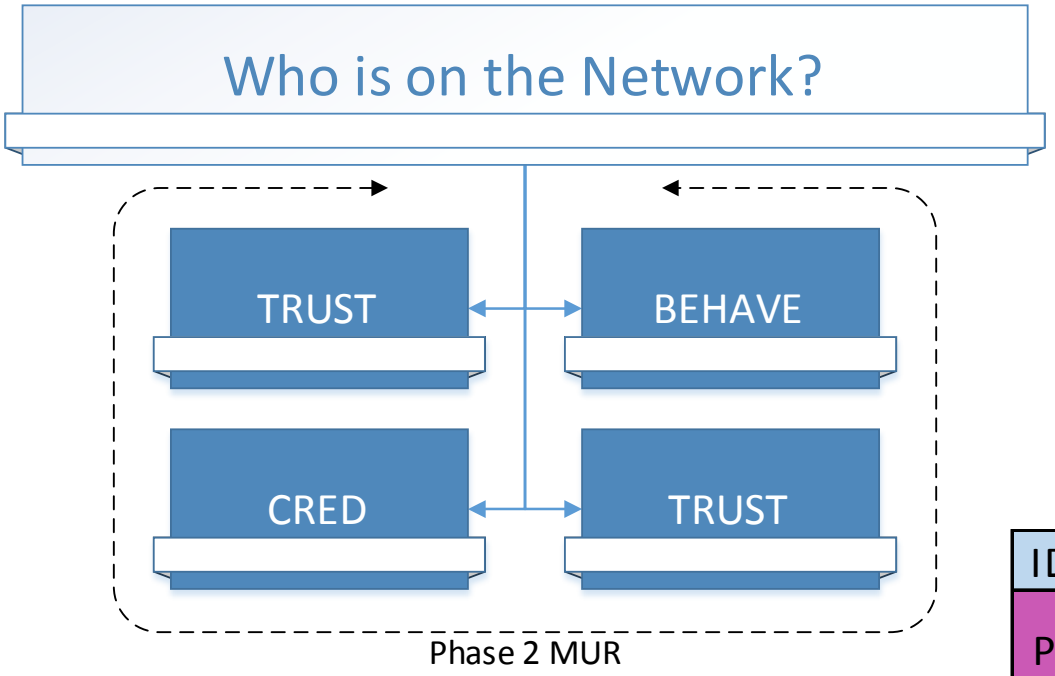


CDM Requirements - "Phase 1"



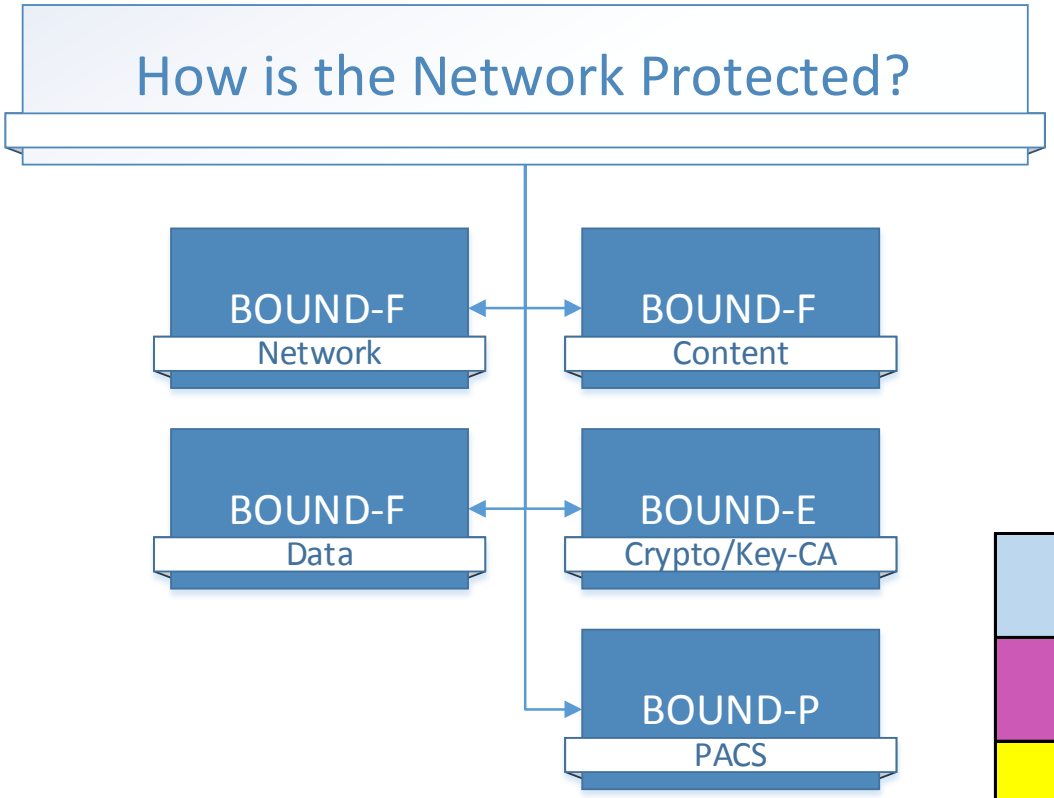
IDENTIFY	Asset Management
	Risk Assessment
PROTECT	Maintenance
	Data Security
DETECT	
RESPOND	
RECOVER	

CDM Requirements – “Phase 2”



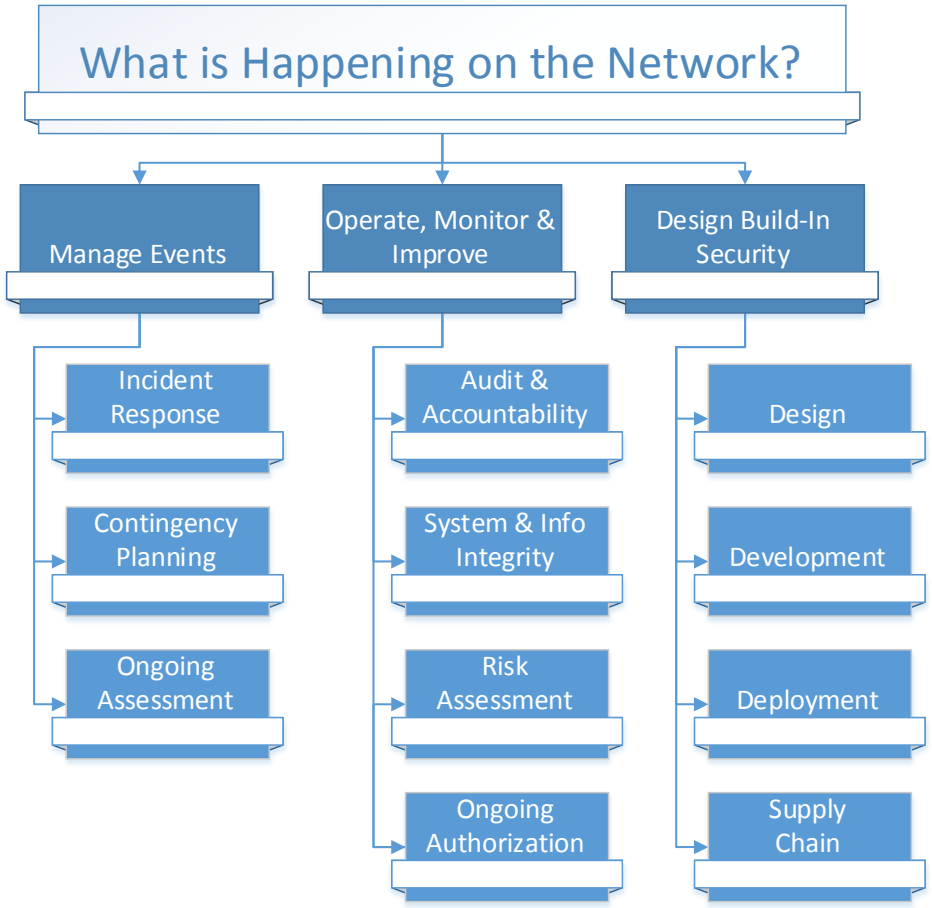
IDENTIFY	Asset Management
PROTECT	Access Control
	Awareness & Training
DETECT	
RESPOND	
RECOVER	

CDM Requirements – “Phase 3”



IDENTIFY	Asset Management
	Risk Assessment
PROTECT	Infrastructure Protection
	Protection Technology
DETECT	Anomalies & Events
	Detection Process
RESPOND	
RECOVER	

CDM Requirements – “Phase 3”



Manage Events	
IDENTIFY	Governance
	Business Environment
PROTECT	Infrastructure Protection
	Data Security
DETECT	Anomalies & Events
	Continuous Monitoring
	Detection Process
RESPOND	Analysis
RECOVER	

Operate, Monitor & Improve	
IDENTIFY	
PROTECT	
DETECT	
RESPOND	Analysis
	Communications
	Improvement
	Mitigation
	Response Plan
RECOVER	Recovery Plan
	Improvement

CDM Requirements - “Phase 4”

Primary Focus areas for Phase 4 would:

- Adds “What Data is on the Network?”
- Adds new security paradigm requirements

Questions?