

Continuous Diagnostics and Mitigation **Webinar Series**

COVER YOUR ASSETS

*What You Need to Know About the
Readiness & Planning Guide for
Asset-Based Security Capabilities*



A CDM Learning Community Webinar
April 14, 2016



**Homeland
Security**

Introduction

- Asset-Based CDM Security Capabilities Overview
- Readiness and Planning (R&P) Guide for Asset-Based CDM Security Capabilities Overview
- What is Implementation Readiness?
- Relationship to NIST CSF
- R&P Terms Explained
- Samples of Foundational and Asset-Based Security Capability Considerations with Examples
- Questions and Answers



CDM PMO Program Managers

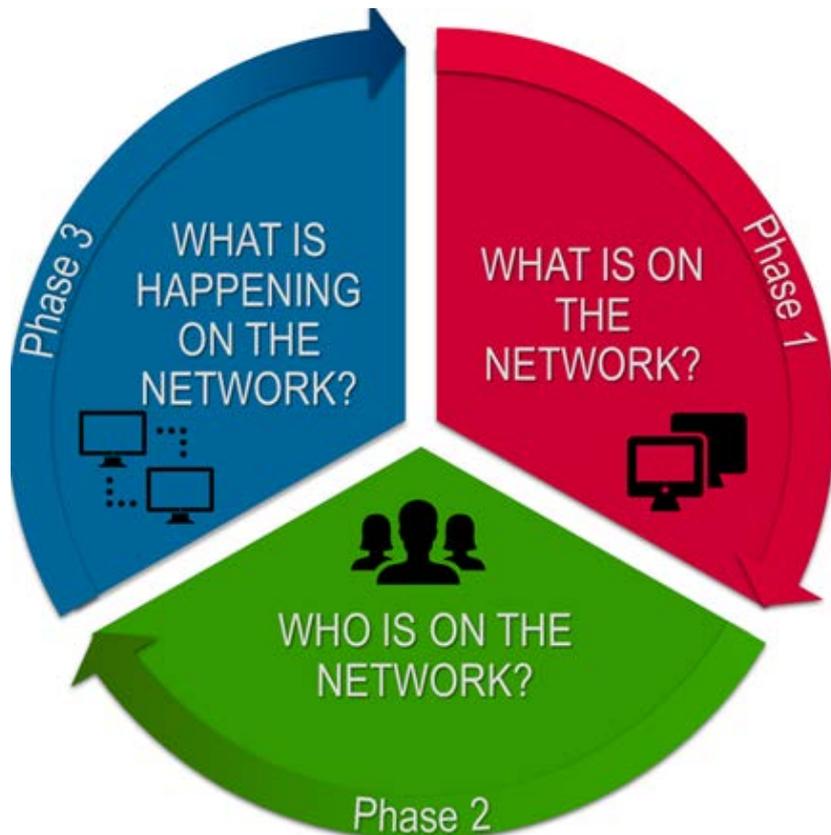
No discussion or questions regarding CDM acquisition or procurement activities – this is strictly a CDM learning community activity. For agency-specific queries, contact:

- **Group A – DHS**
 - Betsy Proch (betsy.proch@hq.dhs.gov)
- **Group B – DOE, DOI, DOT, USDA, VA, OPM**
 - Derrick Williams (derrick.Williams@hq.dhs.gov)
- **Group C – DOC, DOJ, DOL, State, USAID**
 - Paul Loeffler (paul.loeffler@hq.dhs.gov)
- **Group D – GSA, HHS, NASA, SSA, Treasury, USPS**
 - Odell Blocker (odell.blocker@hq.dhs.gov)
- **Group E – Educ, EPA, HUD, NRC, NSF, SBA**
 - Derek Adams (derek.adams@hq.dhs.gov)
- **Group F – Non-Chief Financial Officer (CFO) Act Agencies**
 - Geri Clawson (geraldine.clawson@hq.dhs.gov)
- **Unsure?**
 - cdmlearning@hq.dhs.gov



Homeland
Security

Focus of Asset-Based Security Capabilities



What is on the Network?

HWAM

SWAM

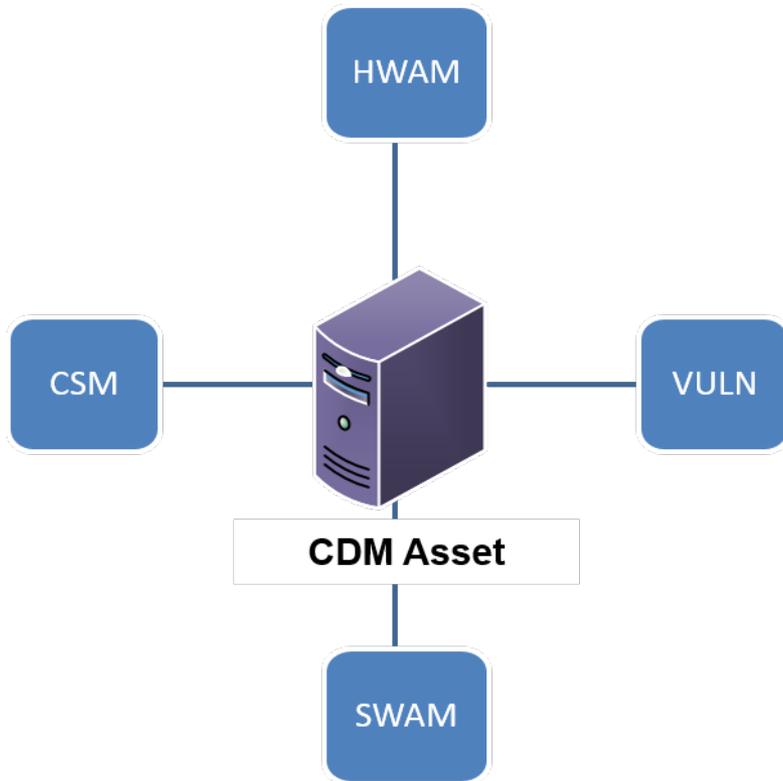
CSM

VULN



Homeland
Security

Asset-Based CDM Security Capabilities Overview



HWAM

- Find all addressable Devices
- Authorization?
- Risk Manage Differences

SWAM

- SW Baseline
 - O/S
 - Common
 - Specific
- Fingerprint
- Authorization?

CSM

- Baseline
- Policy variance
- Authorization?
- Risk Manage Differences

VULN

- Detect
- Score
- Characteristics



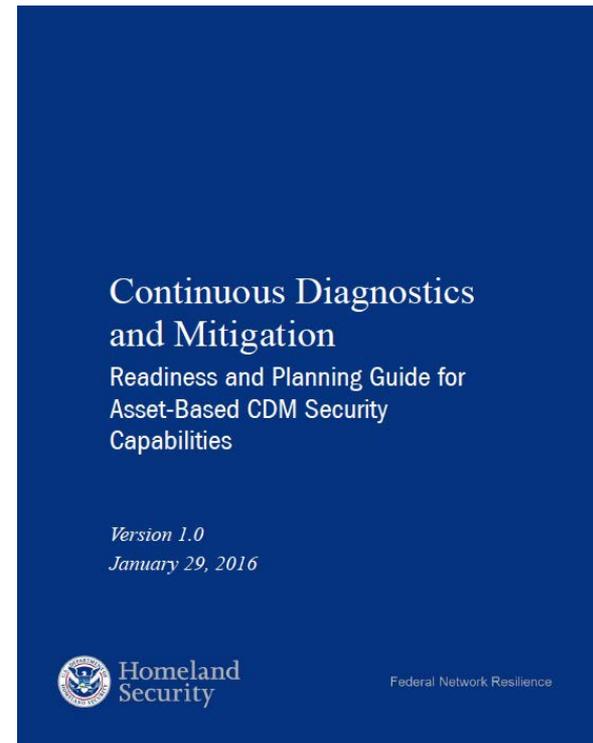
Readiness & Planning Guide for Asset-Based CDM Security Capabilities

The Asset-Based R+P Guide:

Identifies **foundational practices** common to all Asset-Based CDM Security Capabilities

Describes **capability-specific practices** supportive to implementation readiness of each Asset-Based CDM Security Capability

Provides a set of **readiness considerations** to support discussion with the CMaaS Provider either before or during implementation



Homeland
Security

What is Implementation Readiness?

- **Implementation Stage** – “The objective of the Implementation stage is to prepare the system, **operational environment**, **organization**, and **users** for the intended use of the new solution...”¹
- Definition of readiness
 - read·i·ness 'redēnəs/
 - noun: **readiness**
 - 2. the state of being fully **prepared** for something
- Asset-Based CDM Security Capability Implementation Readiness is the state in which the **operational environment**, **organization**, and **users are prepared to implement Asset-Based CDM Security Capabilities**.

¹ Interim Release of Systems Engineering Lifecycle Guide (ver. 2.0). 9/21/2010. Department of Homeland Security.



Relationship to the NIST Cybersecurity Framework

The R&P Guide for Implementing CDM Asset-Based Capabilities identifies a *Cybersecurity Framework* subcategory to represent a foundational and capability-specific practice

Functions	Categories	Subcategories	Informative References
IDENTIFY			
PROTECT			
DETECT			
RESPOND			
RECOVER			

Framework Core Structure



Homeland
Security

R&P Definitions

Business Practice

is method, procedure, process, or rule employed or followed by a company in the pursuit of its objectives. Business practice may also refer to these collectively.²

Foundational Practices

are those practices **common** to two or more CDM asset-based security capabilities.

Capability-Specific Practices

are those practices **unique** to a specific CDM asset-based security capability.

Considerations are intended to help an organization **self-identify** business processes and management activities necessary for CDM asset-based implementation

² <http://www.businessdictionary.com/definition/business-practice.html#ixzz44UikbDgB>



Foundational Practice 1

- **“Information Security roles and responsibilities are coordinated and aligned with internal roles and external partners.”**
 - *Example: An organization has CDM coordination between the OCIO and IA, and O&M is included in CDM working groups. Designated personnel have been assigned, and the working groups have the technical experience needed (IT O&M), as well as the security requirements for onboarding CMaaS providers (HR, Security).*



HWAM Practice 1

- **“All authorized devices (i.e., hardware assets) are in the hardware asset inventory.”**
 - *Example: An organization has a few spreadsheets (some known to be outdated) which are centralized and which represent the approved inventory. Assets are centrally and uniquely identified across the organization. There is a hardware authorization process and it does take into account previously identified devices that reappear on the network for extended periods of time.*



HWAM Practice 2

- **“Only authorized hardware assets are allowed to be on the network.”**
 - *Example: An Agency uses a software application to monitor the use of removable flash media to ensure security and control of their networks. Any unauthorized media is flagged by the system and subject to review by system administrators.*



Homeland
Security

HWAM Practice 3

- **“All authorized hardware assets have a manager assigned to them.”**
 - *Example: Each system within a D/A should be under the responsibility of an Information System Owner. Details of the responsibilities of a system owner can be found in the CDM Roles and Responsibilities Guide and should be updated and tracked within a timeframe prescribed by the organization.*



Homeland
Security

SWAM Practice 1

- **“Software platforms and applications within the organization are inventoried.”**
 - *Example: An organization has spreadsheets of OS on desktops, and a list of all applications on devices on the network. There is an authorization process for desktop baselines, and the inventory is validated for accuracy. The scope of multiple software inventories is validated across the network, and the pace of the central authorization process does hold up business efforts.*



Homeland
Security

SWAM Practice 2

- **“Malicious Code is detected.”**
 - *Example: An organization has antivirus installed on endpoints when their baselines are built, and malicious code prevention is actively configured. Whitelisted processes and applications may be configured on the devices to prevent other processes and applications from initiating.*



Homeland
Security

SWAM Practice 3

- **“Integrity checking mechanisms are used to verify software, firmware, and information integrity.”**
 - *Example: An organization uses Software Identification tags to accurately manage and maintain software within their centralized inventory as well as to detect software assets.*



Homeland
Security

CSM Practice 1

- **“The development and testing environment(s) are separate from the production environment.”**
 - *Example: An organization has some software tests performed at contractor facilities, but most testing takes place in production on its operational network. This is a risk to the operational systems, but it is accepted as necessary for business to continue as normal.*



Homeland
Security

CSM Practice 2

- **“A baseline configuration of information technology/industrial control systems is created and maintained.”**
 - *Example: An organization has a baseline IT group, which is a continuous process that takes place when new OS are built and only on OS or software that is in the initial OS build (IE, Outlook). Validation of those baselines is performed in production and during network use.*



Homeland
Security

CSM Practice 3

- **“Configuration change control processes are in place.”**
 - *Example: An organization has change control process and System Development Life Cycle (SDLC) policy. When new IT is brought in, those processes focus on maintaining high levels of security while delivering business solutions to customers on time. Larger acquisitions typically have more testing performed as resources are available.*



Homeland
Security

VULN Practice 1

- **“Threat and vulnerability information is received from information sharing forums and sources.”**
 - *Example: Organizations utilize services such as the Common Vulnerability Scoring System to understand new threats present in the cyber environment.*



Homeland
Security

VULN Practice 2

- **“A vulnerability management plan is developed and implemented.”**
 - *Example: An organization scans for vulnerabilities, based off of its vulnerability management policy which includes network scope, responsibilities, frequency, or integration with patch management processes for risk mitigation.*



Homeland
Security

VULN Practice 3

- **“Vulnerability scans are performed.”**
 - *Example: D/As use vulnerability scanners to search for software flaws (IE unpatched software) to perform consistent scans of their systems in order to combat cyber threats from impacting their networks.*



Homeland
Security

Summary

- Asset-Based CDM Security Capabilities Overview
- Readiness and Planning (R&P) Guide for Asset-Based CDM Security Capabilities Overview
- What is Implementation Readiness?
- Relationship to NIST CSF
- R&P Terms Explained
- Samples of Foundational and Asset-Based Security Capability Considerations with Examples



Additional Resources

GSA Site

- <http://www.gsa.gov/cdm>

US-Cert Site

- <http://www.us-cert.gov/cdm>

Additional Upcoming Activities

- April 27, 2016
 - CDM Learning Community Event
CDM: An Introduction and Overview of the DHS CS&C NPPD
FNR Activities: Supporting Federal Cybersecurity Programs
Time: 11:00 am – 1:00 pm
Location: AvayaLive Engage and HSIN Connect
Registration Information - <https://www.us-cert.gov/cdm/training>



Homeland
Security

CDM PMO Program Managers

No discussion or questions regarding CDM acquisition or procurement activities – this is strictly a CDM learning community activity. For agency-specific queries, contact:

- **Group A – DHS**
 - Betsy Proch (betsy.proch@hq.dhs.gov)
- **Group B – DOE, DOI, DOT, USDA, VA, OPM**
 - Derrick Williams (derrick.Williams@hq.dhs.gov)
- **Group C – DOC, DOJ, DOL, State, USAID**
 - Paul Loeffler (paul.loeffler@hq.dhs.gov)
- **Group D – GSA, HHS, NASA, SSA, Treasury, USPS**
 - Odell Blocker (odell.blocker@hq.dhs.gov)
- **Group E – Educ, EPA, HUD, NRC, NSF, SBA**
 - Derek Adams (derek.adams@hq.dhs.gov)
- **Group F – Non-Chief Financial Officer (CFO) Act Agencies**
 - Geri Clawson (geraldine.clawson@hq.dhs.gov)
- **Unsure?**
 - cdmlearning@hq.dhs.gov



Homeland
Security

Questions and Answers



Homeland
Security

Survey Questions

- Please help us improve these events by answering the 7 survey questions



Homeland
Security

CUE/CPE Information

- Thanks for attending today's session!
- A generic Webinar completion certificate can be downloaded from the following site:
<https://www.us-cert.gov/sites/default.htm...>
- Hold onto the following:
 - Completion certificate after filling in your name
 - A copy of the email confirmation showing you registered for the Webinar



Homeland
Security

Contact Information

*THANK YOU FOR
ATTENDING OUR
WEBINAR.*

Contact: cdmlearning@hq.dhs.gov



Homeland
Security