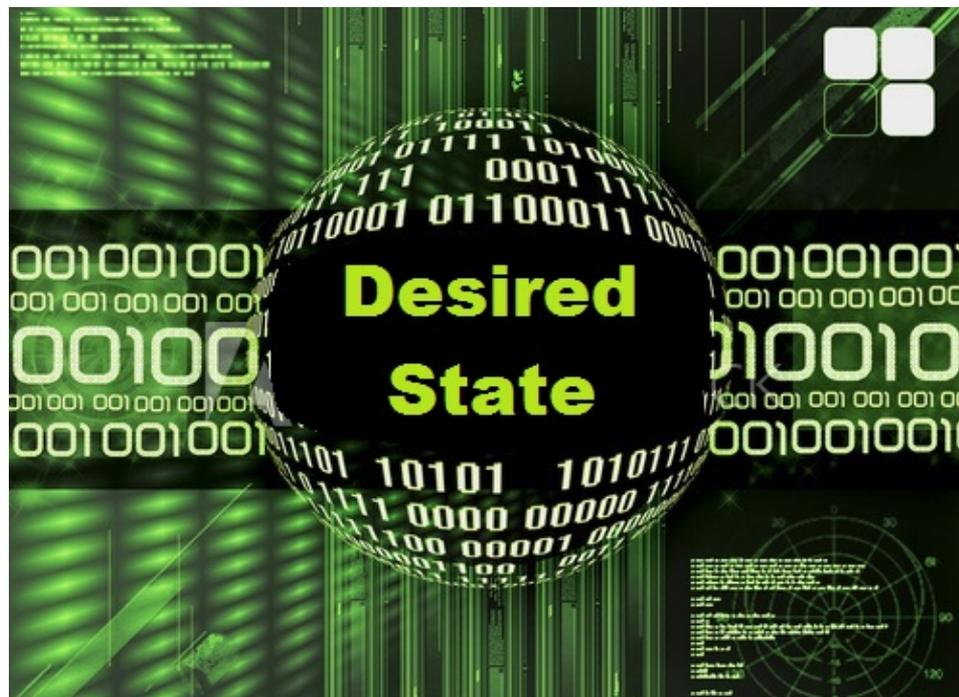


Let's See It: Policy, Desired State, and CDM

January 26, 2017
12:00 pm - 1:00 p.m. EST



A CDM LEARNING COMMUNITY EVENT



Homeland
Security

Federal Network Resilience

Today's Webinar Goals

1

Provide information on what machine-readable policy is and how it relates to desired state specifications.

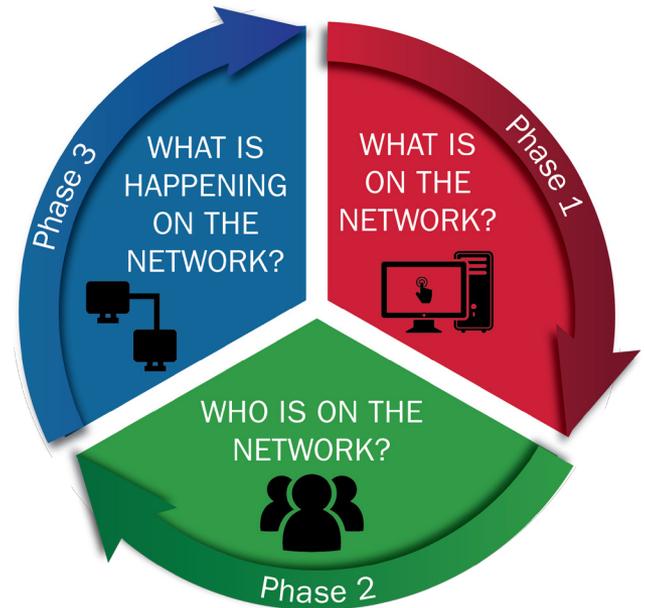
2

Provide examples of how machine-readable policy is entered into CDM.



We'll Answer These Questions

- ▶ What is machine-readable policy (MRP)?
- ▶ How is CDM desired state data entered into the CDM system?
- ▶ What are some CDM desired state examples?



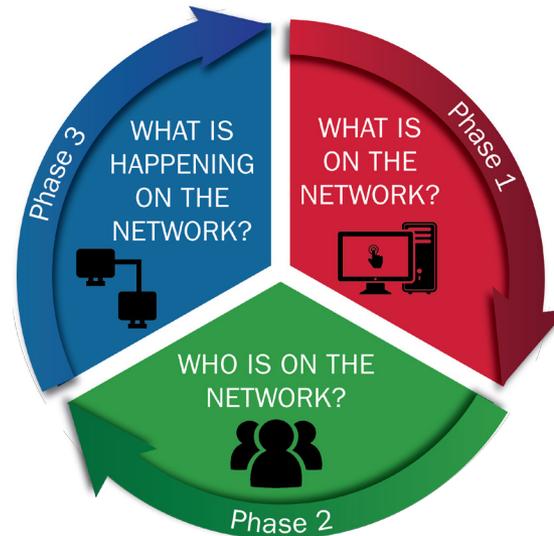
Today's Speaker: Richard M. McMaster

Certified Information Systems Security Professional (CISSP)

- ▶ Implementation Manager for Department of Homeland Security (DHS) implementation of CDM Phase 1 functionality.
- ▶ Senior technical engineer for Network Security Deployment (NSD).
- ▶ Technical subject matter expert for the CDM program at the DHS program level.



What Is Machine-Readable Policy (MRP)?



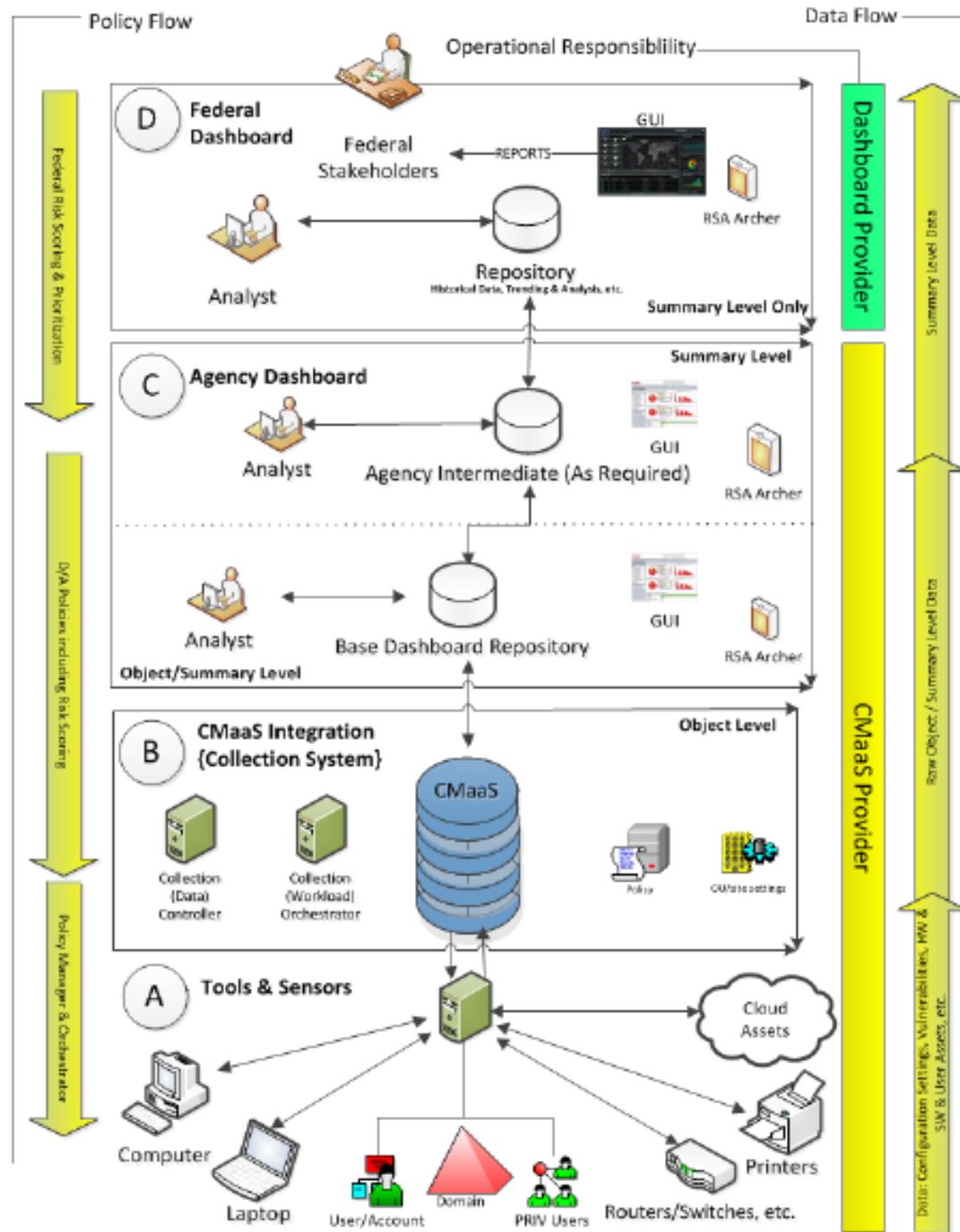
What Is MRP?

- ▶ Federal and/or agency **policy codified into a machine-readable format** to be automatically used by the CDM system.
- ▶ The **desired state**.
- ▶ Format that enables the CDM system to **automatically compare policy to sensor information** (actual state) to determine defects.



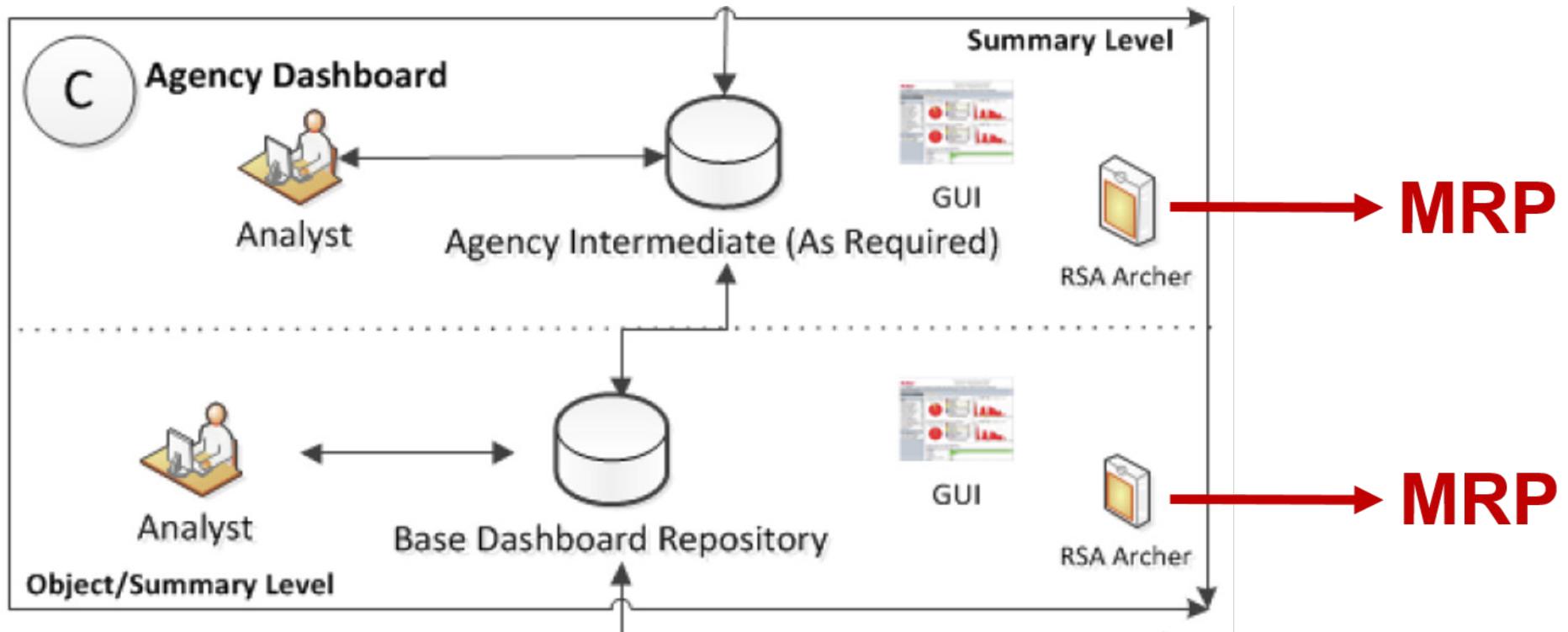
CDM System Architecture

Department of Homeland Security,
 Continuous Diagnostics and Mitigation
 (CDM) System Architecture: Architecture
 Principles Document, 2016, 3.



Homeland Security

Where Does MRP Fit?



What Is Machine-Readable Data?

Data in a format that can be **automatically read and processed** by a computer.

Must be **structured data**.

Examples:

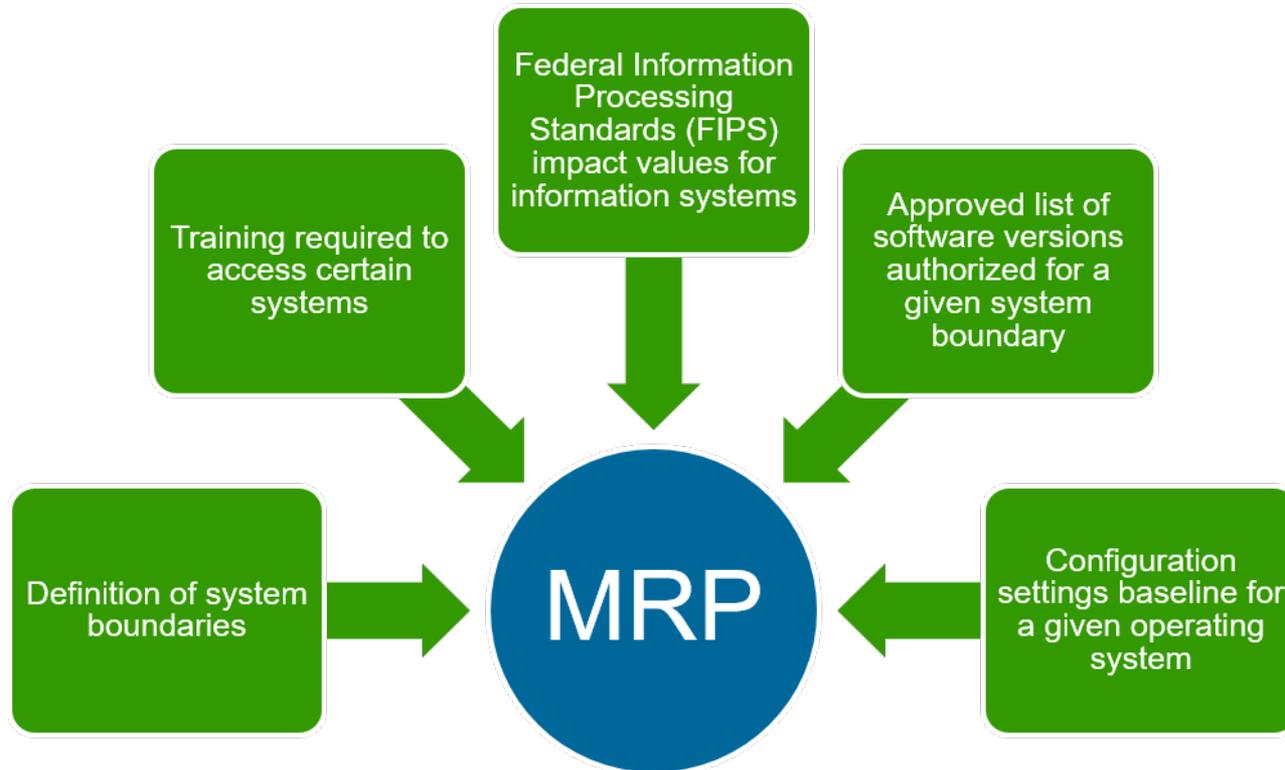
- ▶ Extensible Markup Language (XML)
- ▶ Extensible Configuration Checklist Description Format (XCCDF)
- ▶ Comma-Separated Values (CSV)



```
<?xml version="1.0"
<person id="000000"
  <name>Kris
  <address>
    <street>
    <city>80
```

Example of XML

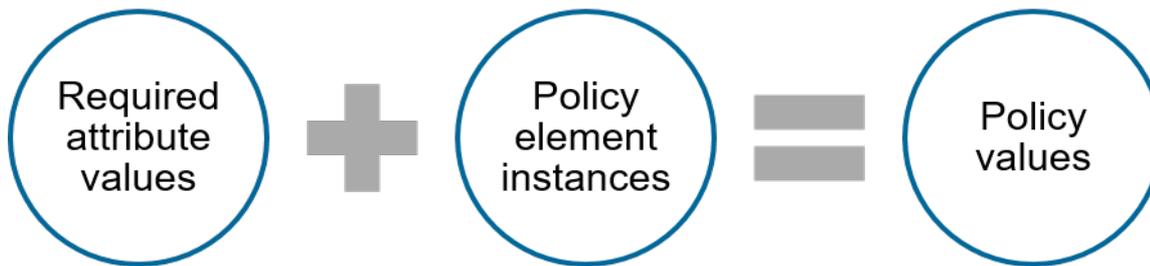
Examples of MRP Elements



Policy Values

The common-schema defines which **policy elements** and **attributes** are required by CDM.

The policy values must be entered into CDM.



Example

MRP Responsibilities: Dashboard and Continuous Monitoring as a Service (CMaaS) Providers

- ▶ Provide mechanisms to **enter MRP elements into CDM** manually, through automated file ingest, and through direct interface to existing agency record systems.
- ▶ Automate mechanisms to **distribute policy elements** defined at higher layers of CDM to lower layers of CDM.
- ▶ Ensure all data necessary to support the common-schema are **collected by or entered into CDM**.
- ▶ Develop automated processes necessary to **normalize data collected by sensors and tools** into the common-schema.

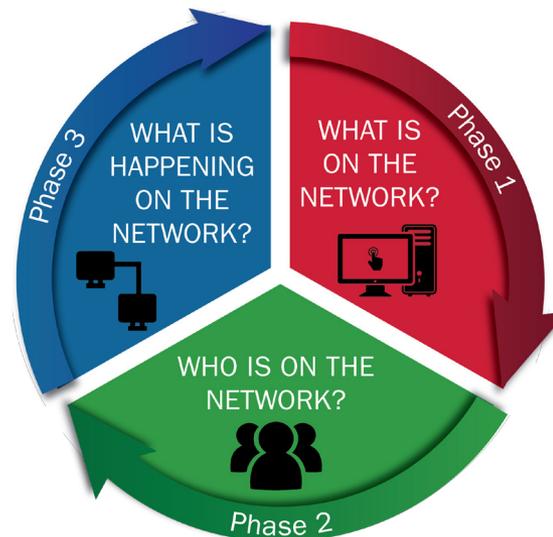


MRP Responsibilities: Agencies

- ▶ Define their **desired security state**.
- ▶ Plan how to **capture or develop the MRP elements** of their desired security state.
- ▶ Make these **MRP elements available to CDM**, including by coordinating with CMaaS providers to integrate existing record systems into CDM.

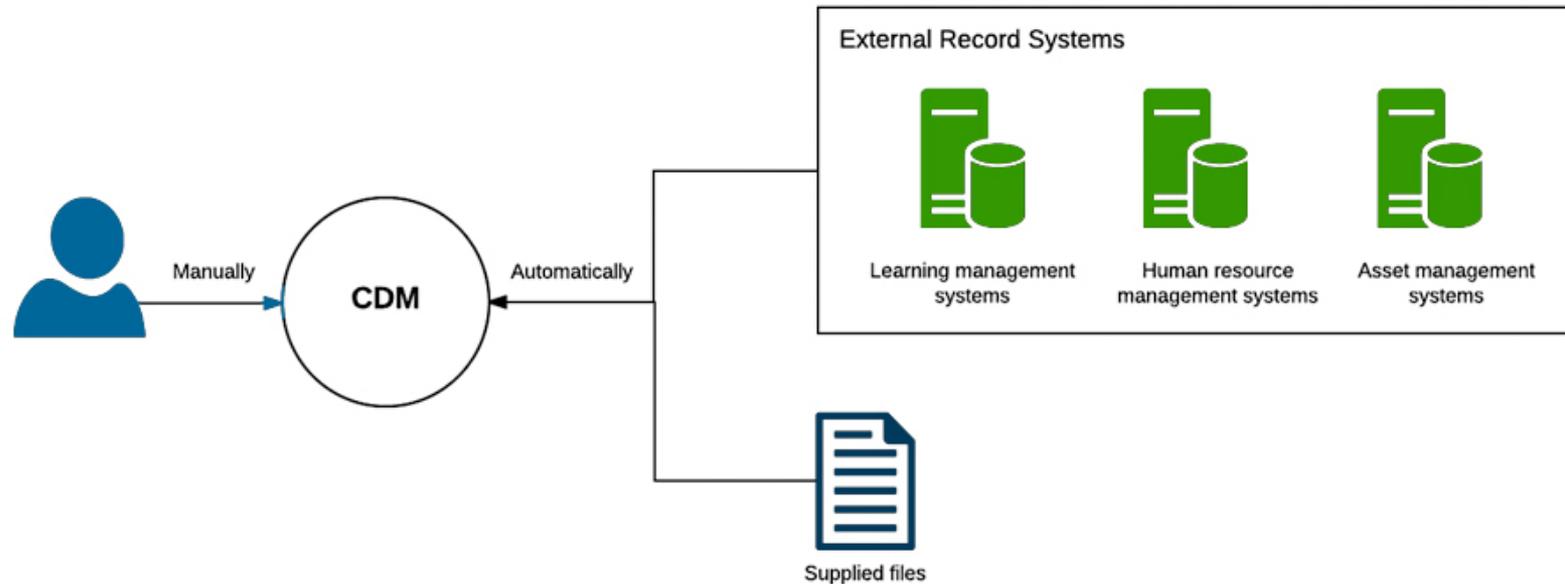


How Is CDM Desired State Data Entered into the CDM System?



How to Enter Desired State Data

The CDM system enables MRP to be entered into CDM either **manually** or **automatically**.

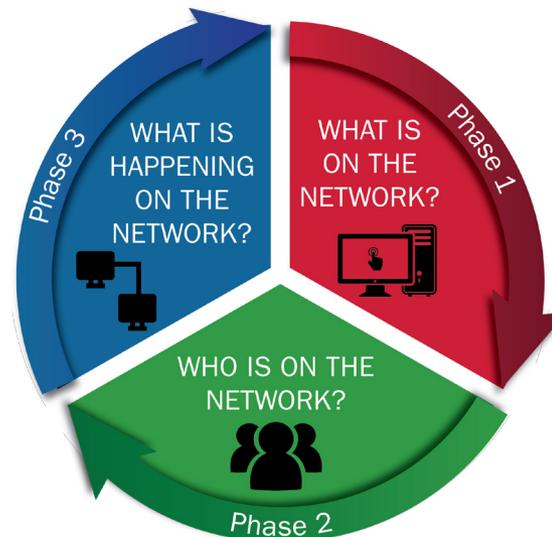


Three Ways Policy Is Added to Archer

- ▶ **Relational** – Example: All hardware assets related to the approved (Federal Information Security Management Act (FISMA)) system are to show as authorized.
- ▶ **Temporal** – Example: Annual security awareness training is completed by a set timeframe.
- ▶ **National Institute of Standards and Technology (NIST) 800-53 Dependency** – Example: When a NIST 800-53 Rev. 4 control indicates the term “agency-dependent” within the control.



What Are Some CDM Desired State Examples?



Hardware Asset Management (HWAM) Desired State Specification Example

Data Item	Justification
<p>Data necessary to accurately identify the device. At a minimum:</p> <ul style="list-style-type: none">• Serial Number• Expected Common Platform Enumeration (CPE) for Hardware or Equivalent<ul style="list-style-type: none">– Vendor– Product– Model Number• Exists in inventory for authorized FISMA system• Other agency requirements as applicable <p>Local enhancements might include data necessary to accurately identify subcomponents.</p>	<p>To be able to uniquely identify the device</p> <p>To be able to validate that the device on the network is the device authorized and not an “imposter”</p>



Software Asset Management (SWAM) Desired State Specification Example

Data Item	Justification
Authorized Software inventory to include assigned and authorized device attributes	To identify what software to check against what defect checks
The associated Value for attributes	To prioritize defects associated with devices
Sets of attributes designated mutually exclusive per the department's/agency's (D/A's) policy	For comparison with the set of assigned attributes for devices
<p>A listing of all authorized software for the D/A to include:</p> <ul style="list-style-type: none"> • Data necessary to accurately identify the software product and compare to actual state data collected <ul style="list-style-type: none"> - Vendor - Product - Version/Release Level/Patch Level - Software Identification Tag (SWID) - CPE • Authoritative listing of executable files associated with the product 	

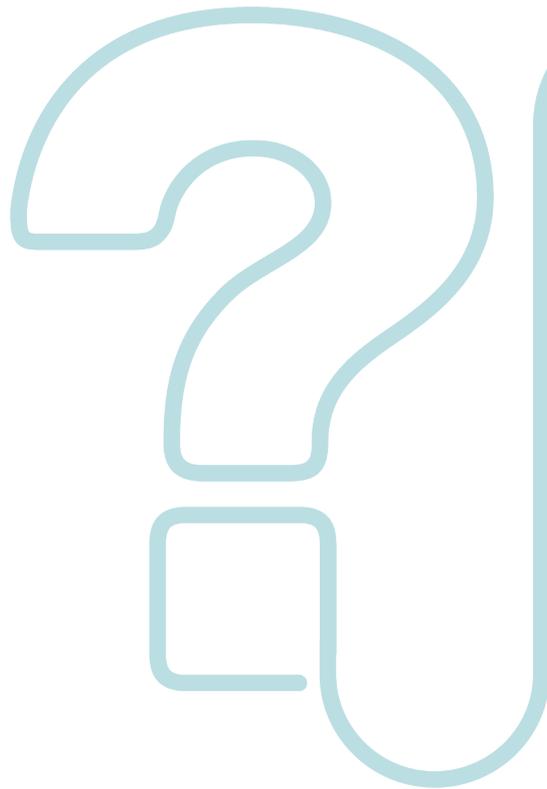


Reference

Department of Homeland Security, Continuous Diagnostics and Mitigation (CDM) System Architecture: Architecture Principles Document, Version 1.0. November 7, 2016.



Audience Question & Answer



Please use the question box on the top right of your screen to ask questions.



Get Involved with the CDM Learning Program!



Visit our website:

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



Engage with our weekly blog:

<https://www.govloop.com/groups/cdm-learning-bits-bytes>



Join our mailing list:

cdmlearning@hq.dhs.gov



Thank You for Attending Today's CDM Webinar!

- ▶ A certificate of attendance will be available to download at www.us-cert.gov/cdm/training within one week of today's event.
- ▶ Please help us provide better learning content by completing the short survey. Your feedback matters!

