Homeland
Security

Continuous Diagnostics and Mitigation (CDM)
Program Update

Martin Stanley
Chief, Cybersecurity Assurance
Office of Cybersecurity and Communications

Unclassified/For Official Use Only (FOUO)

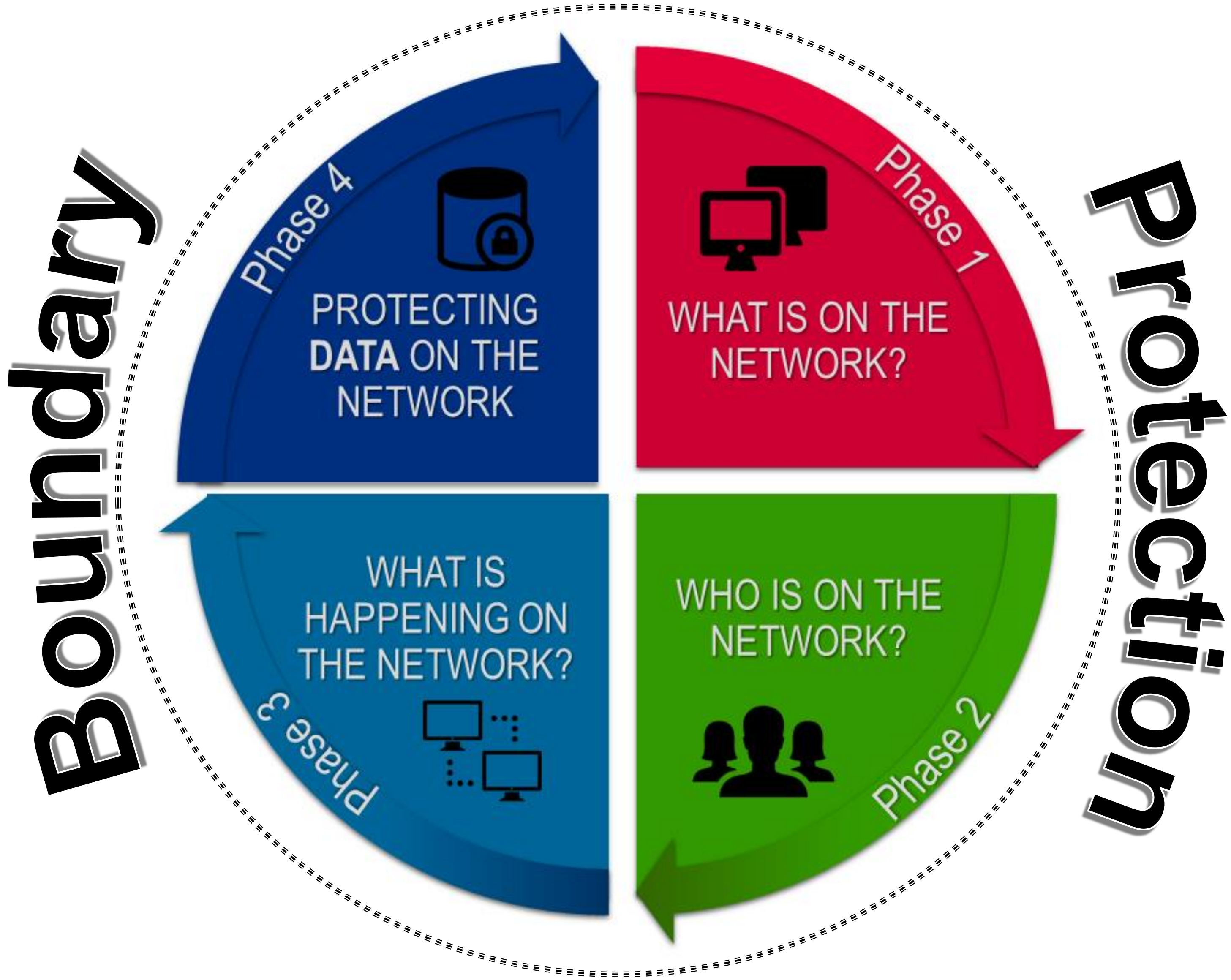
CDM Strategic Program Approach

- Overarching CDM Program Objectives
  - Fix Worst Problems First
  - Strengthen federal networks against attack
- Includes blanket purchase agreements with 17 vendors to provide qualified tools, sensors and integration services
- CDM Capabilities
  - Phased development of requirements based on security control grouping
    - Phase 1 (What is on the Network?)
    - Phase 2 (Who is on the Network?)
    - BOUND (Protecting the boundaries)
    - Phase 3 (What is happening on the Network?)
    - Phase 4 (Protecting the data on the Network)

CDM Orders to Date

- Delivery order in 2014 provided $59.5M in tools and sensors delivering endpoint management and software assurance to 21 civilian agencies
- Task orders awarded in 2015 providing Phase 1 tools, sensors, dashboard and integration services to 25 civilian agencies including 23 Chief Financial Officer Act agencies
- Task order awarded in 2016 providing Phase 2 tools and deployment services to up to 65 agencies

CDM Phases – Strategic View



Boundary

Phase 1

WHAT IS ON THE NETWORK?

Phase 2

WHO IS ON THE NETWORK?

Phase 3

WHAT IS HAPPENING ON THE NETWORK?

Phase 4

PROTECTING **DATA** ON THE NETWORK

Protection

Phase 3 Details

BOUND-F

- Primary focus areas include:
  - Packet Filtering
  - Content Filtering
  - Network Admissions
  - Data Loss/Leak Protection

BOUND-E

- Primary focus areas include:
  - Cryptographic controls
  - Key Management / Certificate Authorities

BOUND-P

- Primary focus areas include: PACS Systems

Phase 3 Details (Cont’d)

Manage Events (MNGEVT)

- Primary focus areas include: event preparation, event sources, and detection and analysis
- Incorporates *Ongoing Assessment*
  - Will require automating the process to monitor, collect, and analyze policy changes, which will capture CDM actual and/or desired state change events

Operate, Monitor, and Improve (OMI)

- Primary focus areas include: audit data collection and analysis; prioritize and resolve; and post incident activity and response
- Incorporates *Ongoing Authorization*
  - Will require automating the process to analyze the events leading to CDM incident risk, and based on the incident analysis, to recommend policy improvements to mitigate future incident threat activity

Design and Build-In Security (DBS)

- Primary focus areas include: trustworthy systems, security weakness and vulnerability, static and dynamic assessment, runtime instrumentation and analysis, and residual risk assessment
- Incorporates *Supply Chain Risk Management*

CDM Objectives for Phase 4

- Recent data breaches heightened the focus on protecting sensitive data
- Defense in depth requires multi-faceted approach, beyond endpoint security
- CDM includes specific data protection capabilities in BOUND as “Data Leak Detection” and “Data at Rest Encryption”
  - Transition from endpoint centric to perimeter and data focus
- Phase 4 OMB recommendations reinforce data focus
  - Augmented Data-Focused Capabilities
    - Digital rights management, data masking, enhanced encryption, enhanced Data Loss Prevention (DLP)
  - Micro-segmentation
  - Mobile Device Management

CDM Agency Dashboard

- The CDM Dashboard vendor, Metrica Team Venture (MTV), competitively procured on behalf of the CDM Program, RSA Archer eGRC to serve as the basis for both the CDM Agency and Federal Dashboards.
- Current RSA Archer eGRC modules (with On-Demand Application provided) in CDM Dashboard:
  - Federal Enterprise Management module
  - Continuous Monitoring module
  - Assessment and Authorization module

CDM Training Program

- Mission: To enhance cybersecurity risk management by fostering a CDM learning environment that increases agency awareness, knowledge, and exchange of best practices.

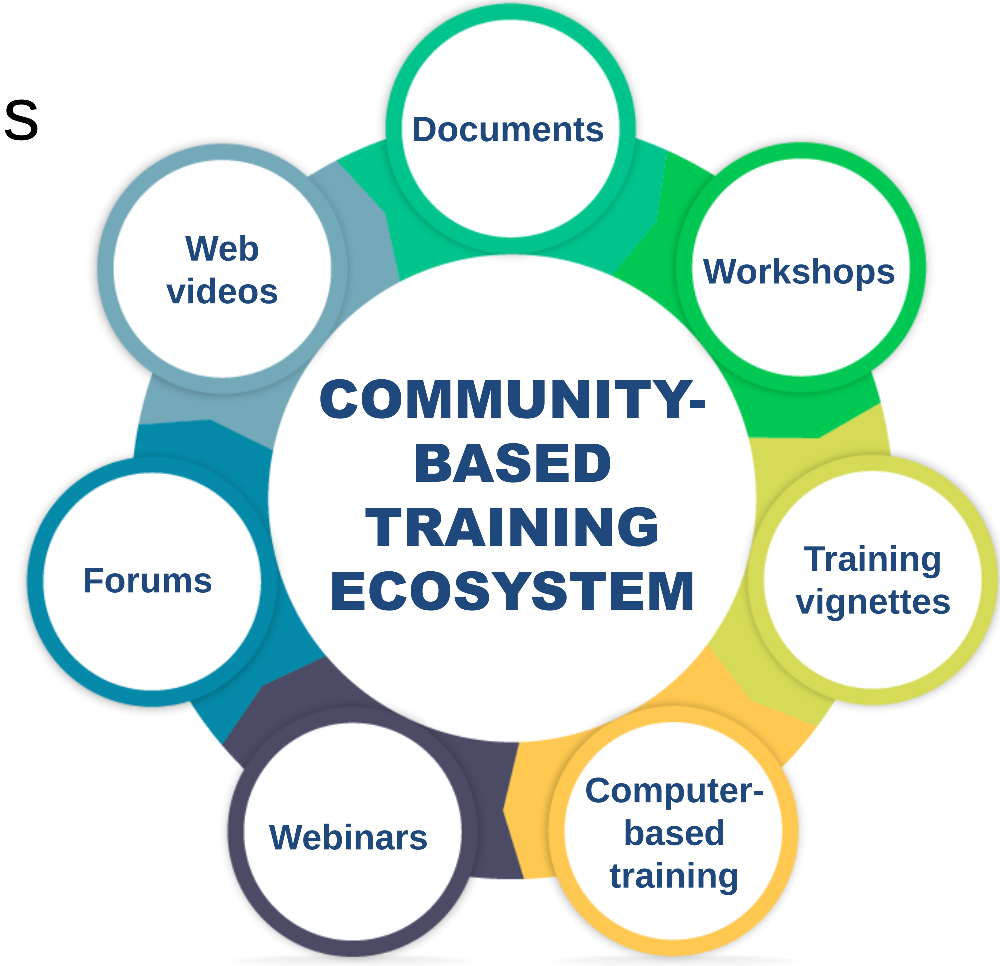
…provide training that will improve understanding of and implementation of the CDM Program.

- Join Distribution List: CDMLearning@hq.dhs.gov
- Visit CDM Training Site: www.us-cert.gov/cdm

CDM Training Program

Current Offerings

- CDM Bits and Bytes
- Monthly Webinar Series
- Monthly Learning Community Events
- Online Vignettes
- Guides



CDM Training Program Overview

During FY16 the DHS learning team:

- Engaged 2,640 partners from the federal civilian enterprise through the webinars and learning community events.
- Issued weekly awareness tips, authored weekly blogs, and conducted monthly training events to socialize the CDM Program’s initial security automation concepts with the intent of raising the level of awareness around how these capabilities can be used to enhance an agencies current cybersecurity efforts.
- Published readiness guides, FAQs, and other learning and awareness materials to prepare agencies for current and future phases of the CDM Program’s activities.

CDM Training Program

CDM Bits and Bytes

WHO: Anyone and everyone

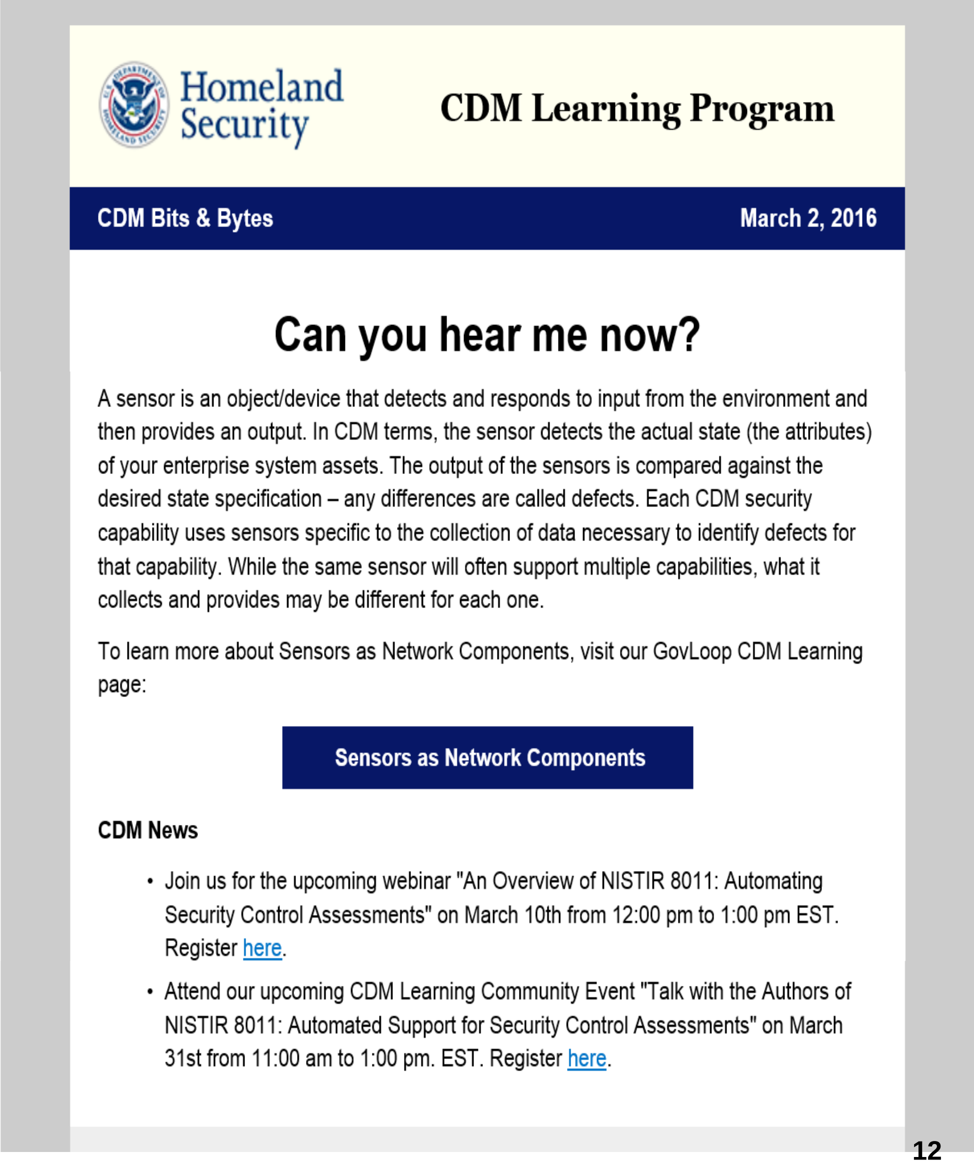
WHAT: Provide information on upcoming news, events, resources, and high level content

WHERE: Via email and blog

WHEN: Every Wednesday

WHY: To understand CDM principles to prepare for planning and implementation.

HOW: GovDelivery and GovLoop



Homeland Security

CDM Learning Program

CDM Bits & Bytes

March 2, 2016

Can you hear me now?

A sensor is an object/device that detects and responds to input from the environment and then provides an output. In CDM terms, the sensor detects the actual state (the attributes) of your enterprise system assets. The output of the sensors is compared against the desired state specification – any differences are called defects. Each CDM security capability uses sensors specific to the collection of data necessary to identify defects for that capability. While the same sensor will often support multiple capabilities, what it collects and provides may be different for each one.

To learn more about Sensors as Network Components, visit our GovLoop CDM Learning page:

CDM News

- Join us for the upcoming webinar "An Overview of NISTIR 8011: Automating Security Control Assessments" on March 10th from 12:00 pm to 1:00 pm EST. Register here.
- Attend our upcoming CDM Learning Community Event "Talk with the Authors of NISTIR 8011: Automated Support for Security Control Assessments" on March 31st from 11:00 am to 1:00 pm. EST. Register here.

CDM Training Program

Monthly Webinar Series

WHO: IT Operations and Mgmt, IT Security

WHAT: One-hour webinar to provide information on CDM topics and related concepts

WHERE: Online

WHEN: 2nd Thursday of each month, 12:00pm – 1:00pm

WHY: Be better prepared for CDM planning and implementation

HOW: Adobe Connect

Past Topics:

April – Getting Started with Your CDM Program

May – Hardware Asset Management

June – Software Asset Management

July/August – Configuration Settings Management

September – Vulnerability Management

October – CDM Phase 2 and Beyond

CDM Training Program

Learning Community Event

WHO: IT Operations and Mgmt, IT Security

WHAT: Online to discuss cybersecurity information and share best practices

WHERE: Online

WHEN: 4th week of each month

WHY: To exchange knowledge, share experiences, create best practices, collaborate, and network

HOW: Adobe Connect

94% of participants agree "the material presented was timely and relevant to my work" (February 2016)

CDM Training Program

Online Vignettes

WHO: IT Operations and Mgmt, IT Security

WHAT: 3 – 8 minutes vignettes explaining CDM core concepts

WHERE: Online

WHEN: Anytime

WHY: Increase baseline knowledge of CDM concepts

HOW: FedVTE and SEI StepFwd platforms

FedVTE:
https://fedvte.usalearning.gov/

FedVTE
FEDERAL VIRTUAL TRAINING ENVIRONMENT
U.S. DEPARTMENT OF HOMELAND SECURITY

CDM Training Program

Guides

WHO: IT Operations and Management, IT Security

WHAT: Training documents with useful recommendations on CDM program implementation and security capabilities

WHERE: Online

WHEN: Anytime

WHY: To help drive intra-agency awareness and solution adoption

HOW: CDM Learning Website: www.us-cert.gov/cdm

Readiness & Planning Guide for Asset-Based CDM Security Capabilities

CDM Roles and Responsibilities

CDM Governance Objectives

Governance activities are focusing on providing agencies transformational support to strengthen cybersecurity-related governance structures and operational management processes to overcome challenges related to CDM tool deployment.

Key CDM Governance Objectives:

- Communicate the importance of a well-defined governance strategy and how it serves as the framework for CDM capabilities
- Support Agencies in the identification of gaps in their cybersecurity governance structures and provide recommendation to close those gaps to support CDM implementation
- Provide clarity around how existing federal standards, policies, and directives can be leveraged to maintain and improve an Agency's Information Security and Continuous Monitoring (ISCM) strategy and program.

Open Discussion

Questions?