

The October CDM Webinar

We will begin at 12:00PM EDT

Welcome to the CDM Webinar: CDM: Transition to Phase Two and Beyond

While you wait, check out:



Our CDM Homepage

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



Our CDM Bits and Bytes Blog

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

Have a topic suggestion for a future event or blog post? Want to join our membership list? Please reach out to cdmlearning@hq.dhs.gov



Homeland
Security

Federal Network Resilience



Homeland Security

CDM: Transition to Phase Two and Beyond

October 13, 2016

12:00 pm – 1:00 pm

A CDM Learning Webinar



Event Goal

The goal is to discuss CDM transitions,
focusing on:

- ▶ CDM Concepts & Design
- ▶ Future Phases
- ▶ What it all means to YOU



CDM Phase 2 and Beyond

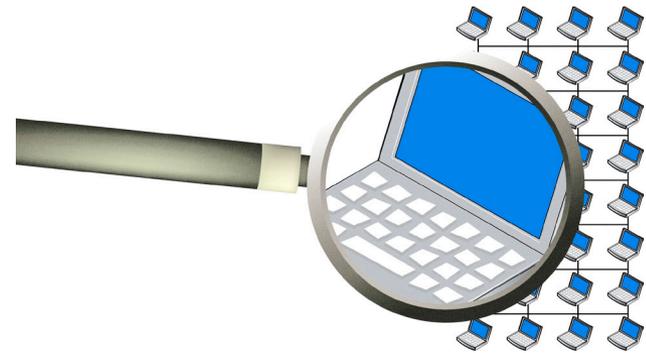
Who is on Your Network?

- ▶ Who are the stakeholders?
- ▶ Who are your users?
- ▶ Do they have proper credentials?



What is Happening on Your Network?

- ▶ Network
- ▶ Encryption
- ▶ Physical Access



Some Questions to Consider

- ▶ What do you need to do to be ready for Phase 2? Phase 3? Beyond?
- ▶ Will your existing processes and tools easily transition to CDM?
- ▶ How do security capabilities differ? How are they related?
- ▶ How will automation help?



Today's Speaker: **Jim Quinn**

Lead System Engineer, Department of Homeland Security CDM Program

- ▶ Primary technical point of contact for \$6B CDM BPA and Dashboard contracts
- ▶ Previously Deputy Chief Technology Officer, DHS National Protection and Programs, Office of the CIO and CISO, DHS Enterprise Services
- ▶ 30+ Years with multiple firms including Alcatel, Cabletron and Digital Equipment Corporation Network and System Development





Continuous Diagnostics and Mitigation (CDM) From Theory to Operations

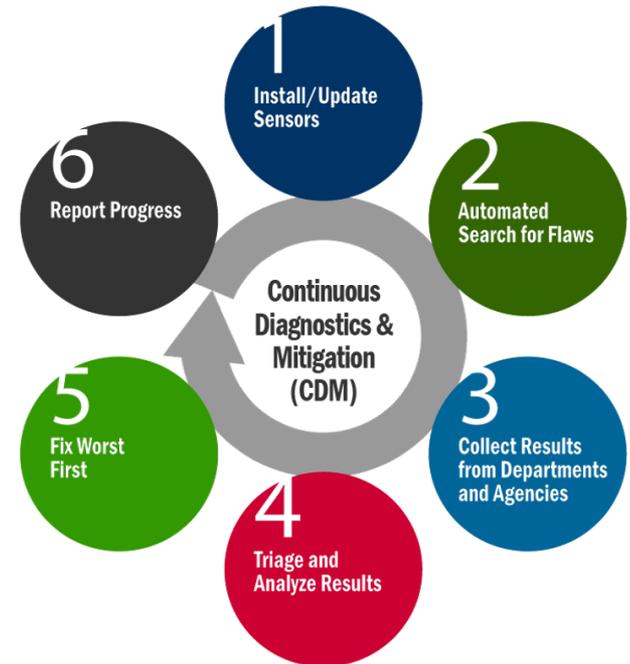
Jim Quinn, October 13, 2016



**Homeland
Security**

CDM Objectives

- Establish consistent, government-wide set of information security continuous monitoring tools to help protect .gov networks
- Leverage the buying power of government organizations to achieve savings for cybersecurity tools and services
- Provide CDM Dashboards to improve situational awareness, and enhance users' ability to identify and respond to emerging cyber threats



Measurement + Metrics

Measures => Realistic Decisions

“Measurement is the first step that leads to control and eventually to improvement. If you can’t measure something, you can’t understand it. If you can’t understand it, you can’t control it. If you can’t control it, you can’t improve it.” — H. James Harrington

Measures cause results

“If a measurement matters at all, it is because it must have some conceivable effect on decisions and behaviour. If we can't identify a decision that could be affected by a proposed measurement and how it could change those decisions, then the measurement simply has no value”

— [Douglas W. Hubbard](#)

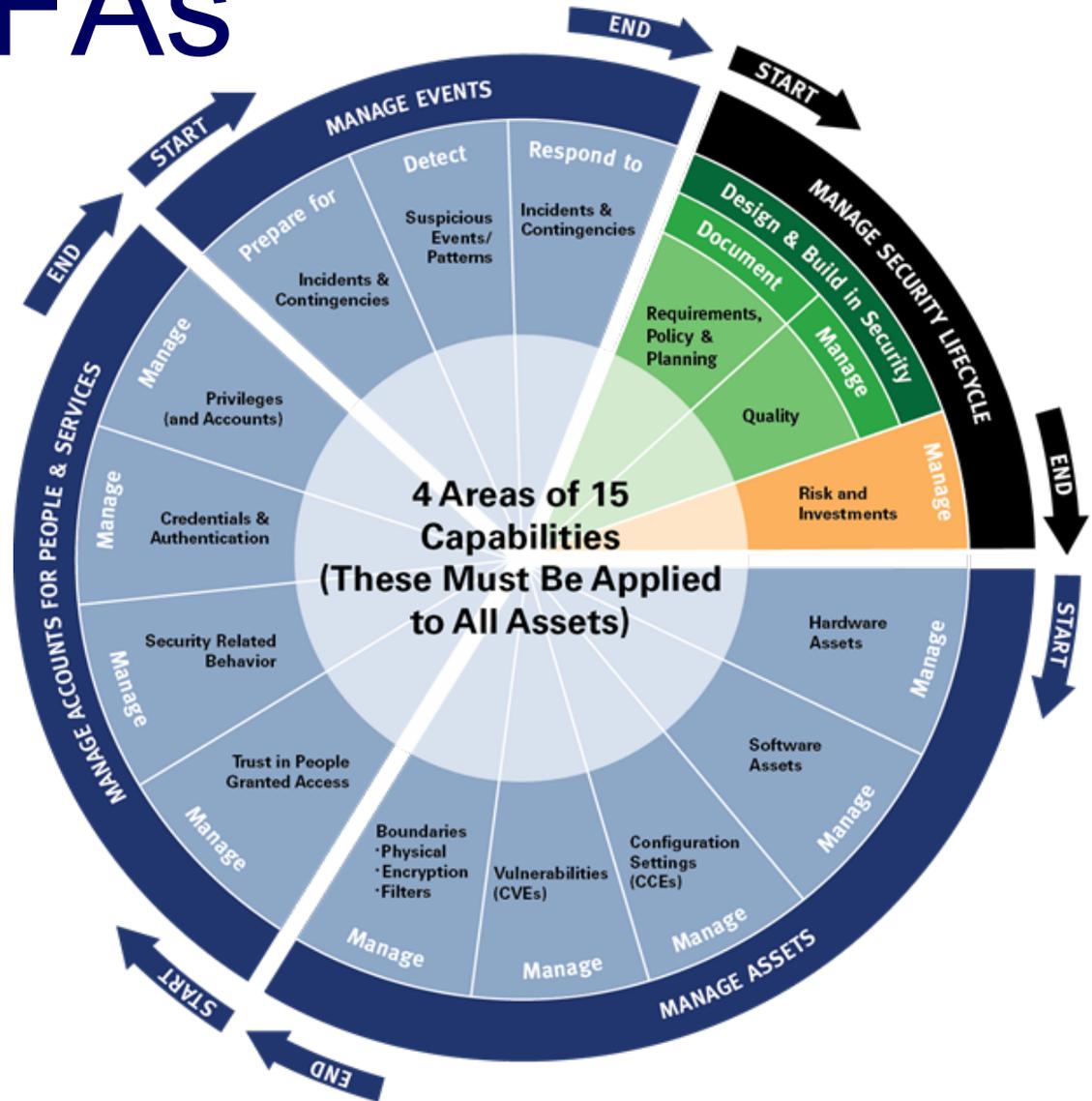


**Homeland
Security**

CDM 15 TFAs

TFA=
Technical
Functional
Areas

They define the
scope of the
CDM Program.



Last Updated 12-Nov-2013



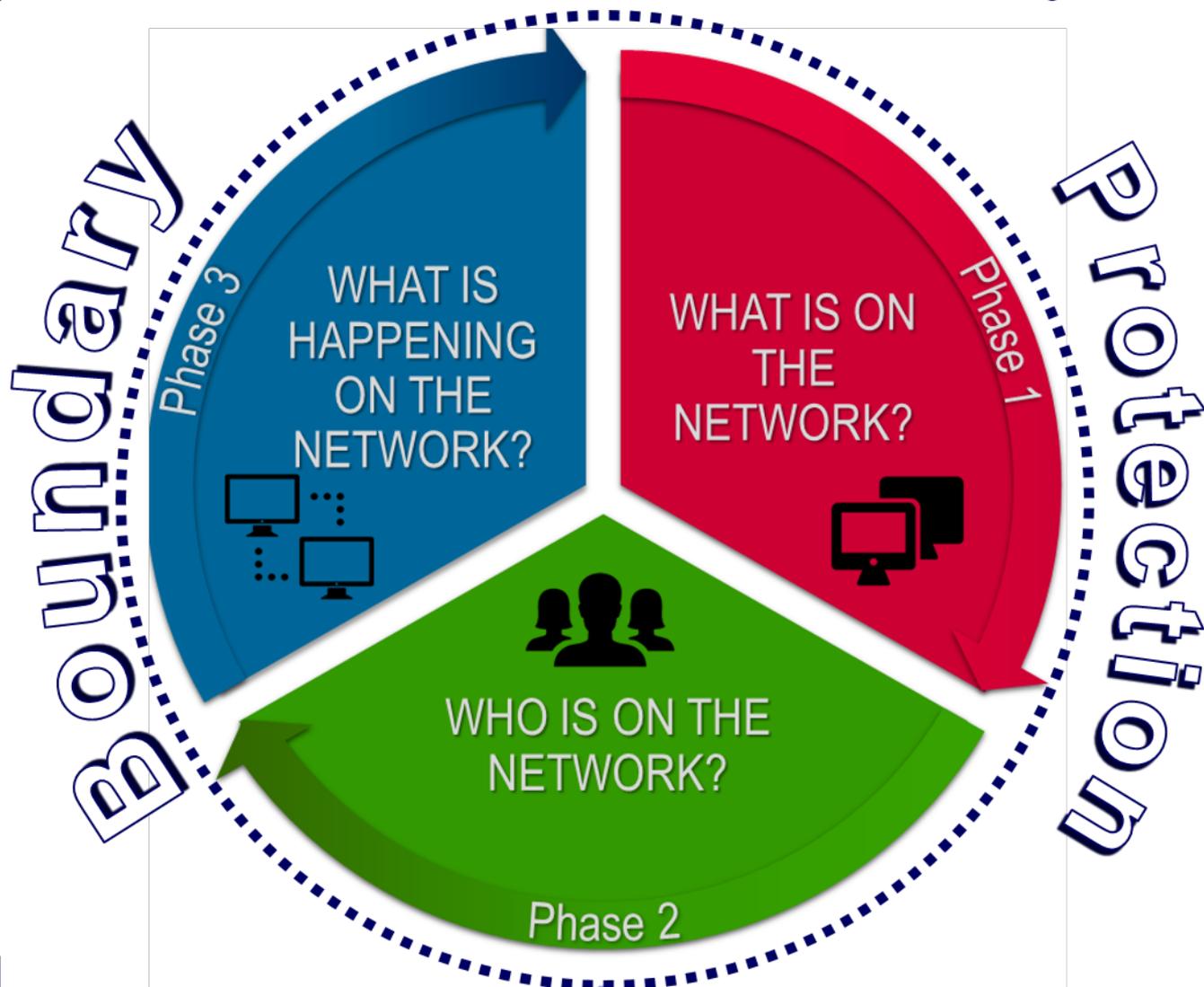
U.S. DEPARTMENT OF
**Homeland
Security**

CDM Capabilities Phased Delivery

Capability:

A collection (set) of security controls that work together to achieve an overall security purpose

NIST 800-53Rev4



**Homeland
Security**

CDM Core Concepts



Dashboard

Risk Scoring

Threat Awareness

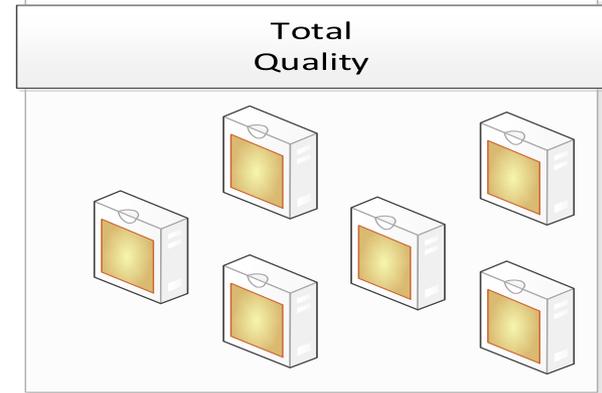
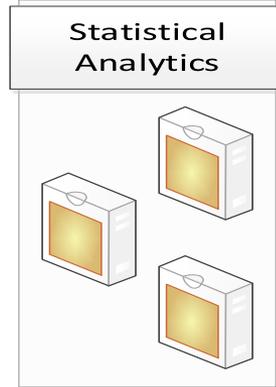
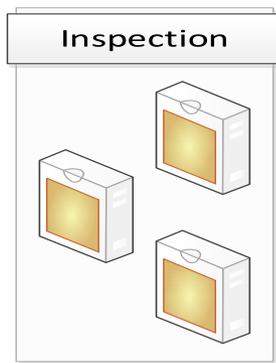
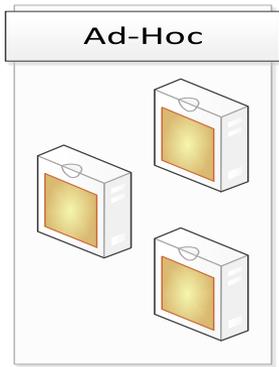
Policy Alerting



Homeland Security

dreamstime.com

Quality Evolution



Homeland
Security

NIST Cybersecurity Framework

The Framework is risk-based, and is composed of three parts: the Framework Core, the Framework Profile, and the Framework Implementation Tiers.

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	ID.AM.1: Physical devices and systems within the organization are inventoried	<ul style="list-style-type: none"> CCS CSC 1 COBIT 5 BAI09.01, BAI09.02 ISA 62443-2-1:2009 4.2.3.4 ISA 62443-3-3:2013 SS.7.8 ISO/IEC 17001:2013 A.8.1.1, A.8.1.2 NIST SP 800-53 Rev. 4 CM-8
		ID.AM.2: Software platforms and applications within the organization are inventoried	<ul style="list-style-type: none"> CCS CSC 2 COBIT 5 BAI09.01, BAI09.02, BAI09.05 ISA 62443-2-1:2009 4.2.3.4 ISA 62443-3-3:2013 SS.7.8 ISO/IEC 17001:2013 A.8.1.1, A.8.1.2 NIST SP 800-53 Rev. 4 CM-8
		ID.AM.3: Organizational communication and data flows are mapped	<ul style="list-style-type: none"> CCS CSC 1 COBIT 5 DSS05.02 ISA 62443-2-1:2009 4.2.3.4 ISO/IEC 17001:2013 A.13.2.1 NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8
		ID.AM.4: External information systems are cataloged	<ul style="list-style-type: none"> COBIT 5 APO02.02 ISO/IEC 17001:2013 A.11.2.6

TIER 1
Partial

Tier 2
Risk Informed

Tier 3
Repeatable

TIER 4
Adaptive



Homeland Security

CDM Architecture Reflects Commercial Best Fit

Approach aligns with Federal procurement practices on COTS

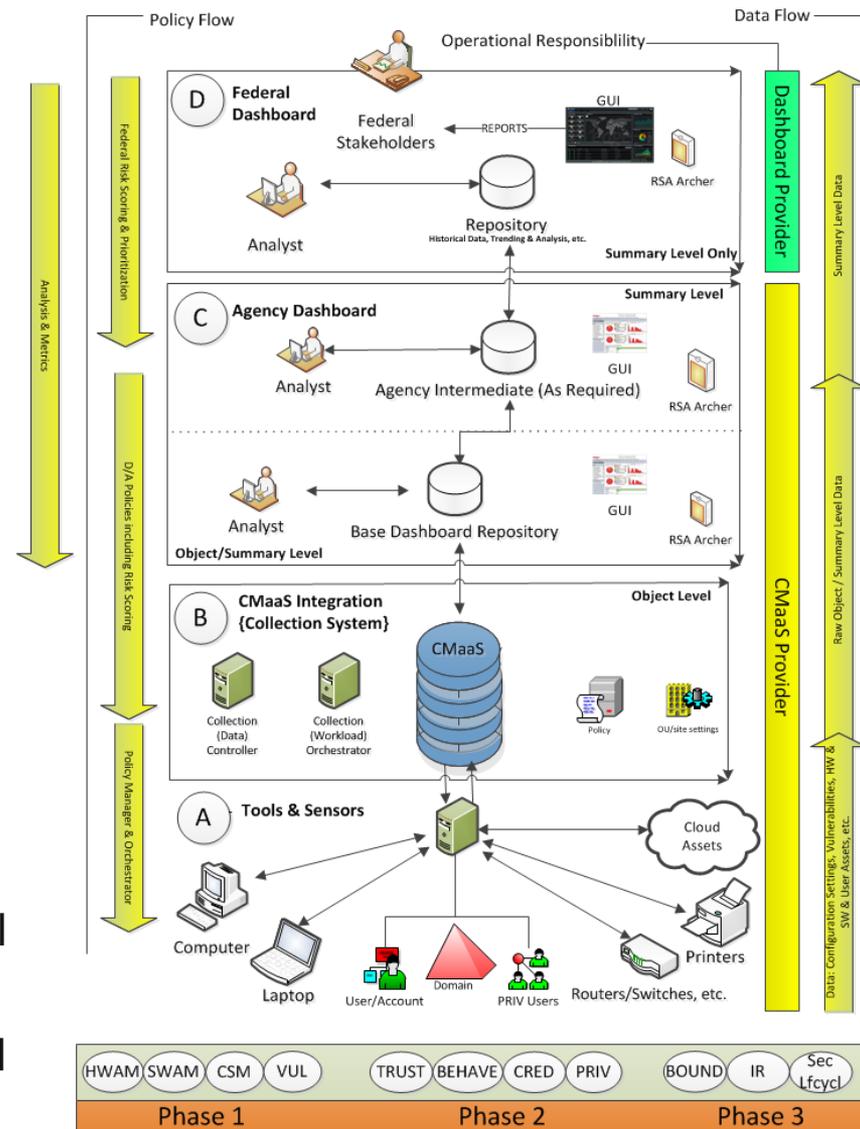
- Per Title 44 USC §3551: key role of COTS

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

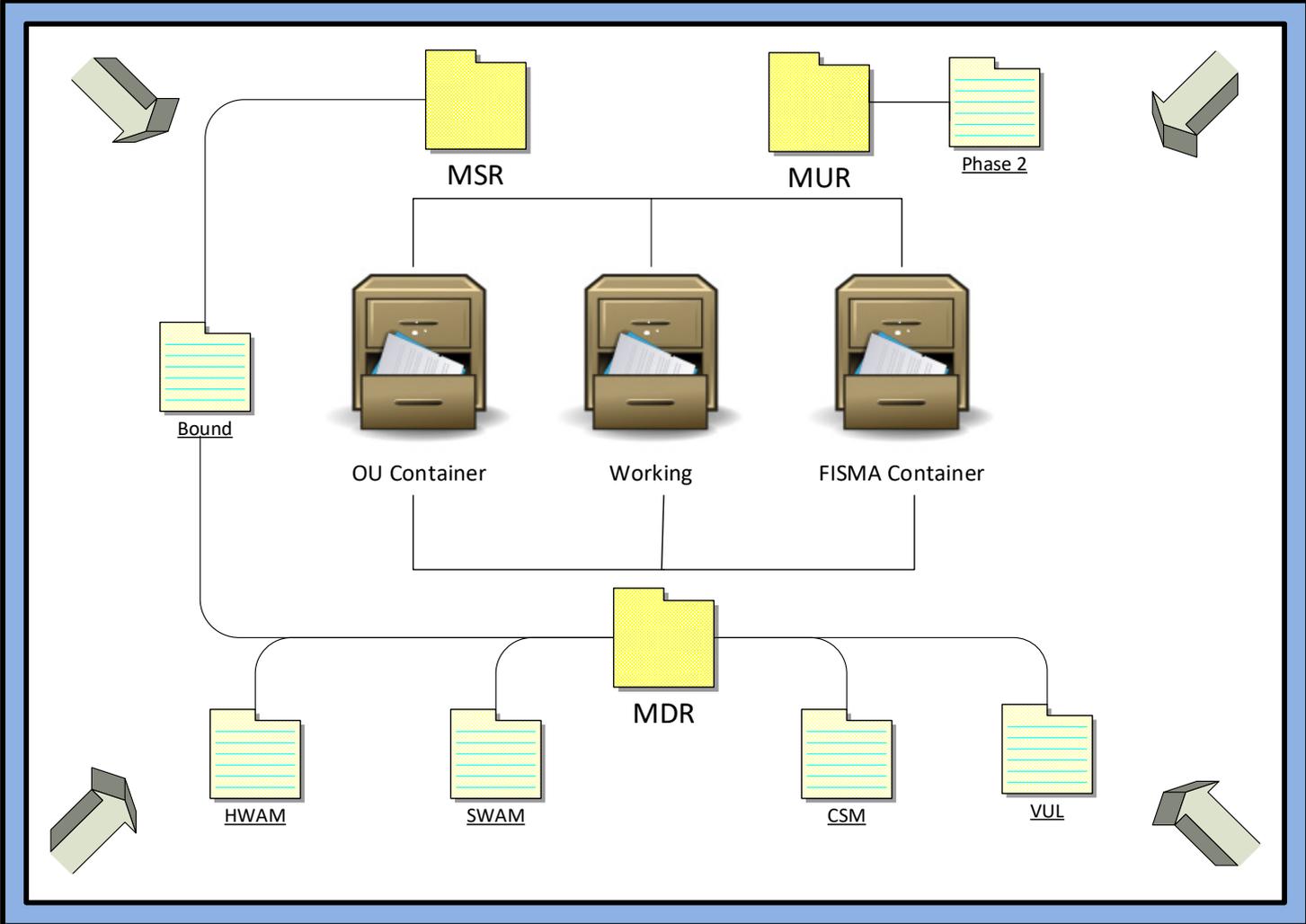


U.S. DEPARTMENT OF
HOMELAND SECURITY

Homeland Security

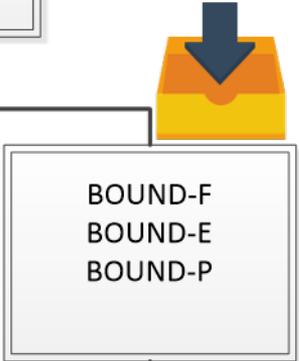
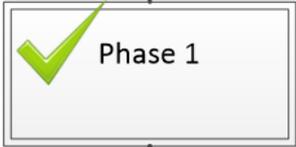
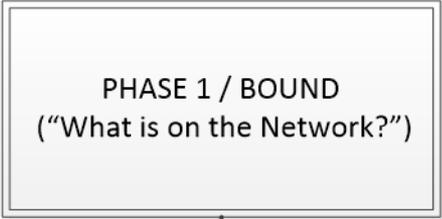
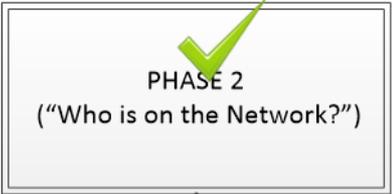
CDM Data Model

Tools and Sensors (Metrics and Events)

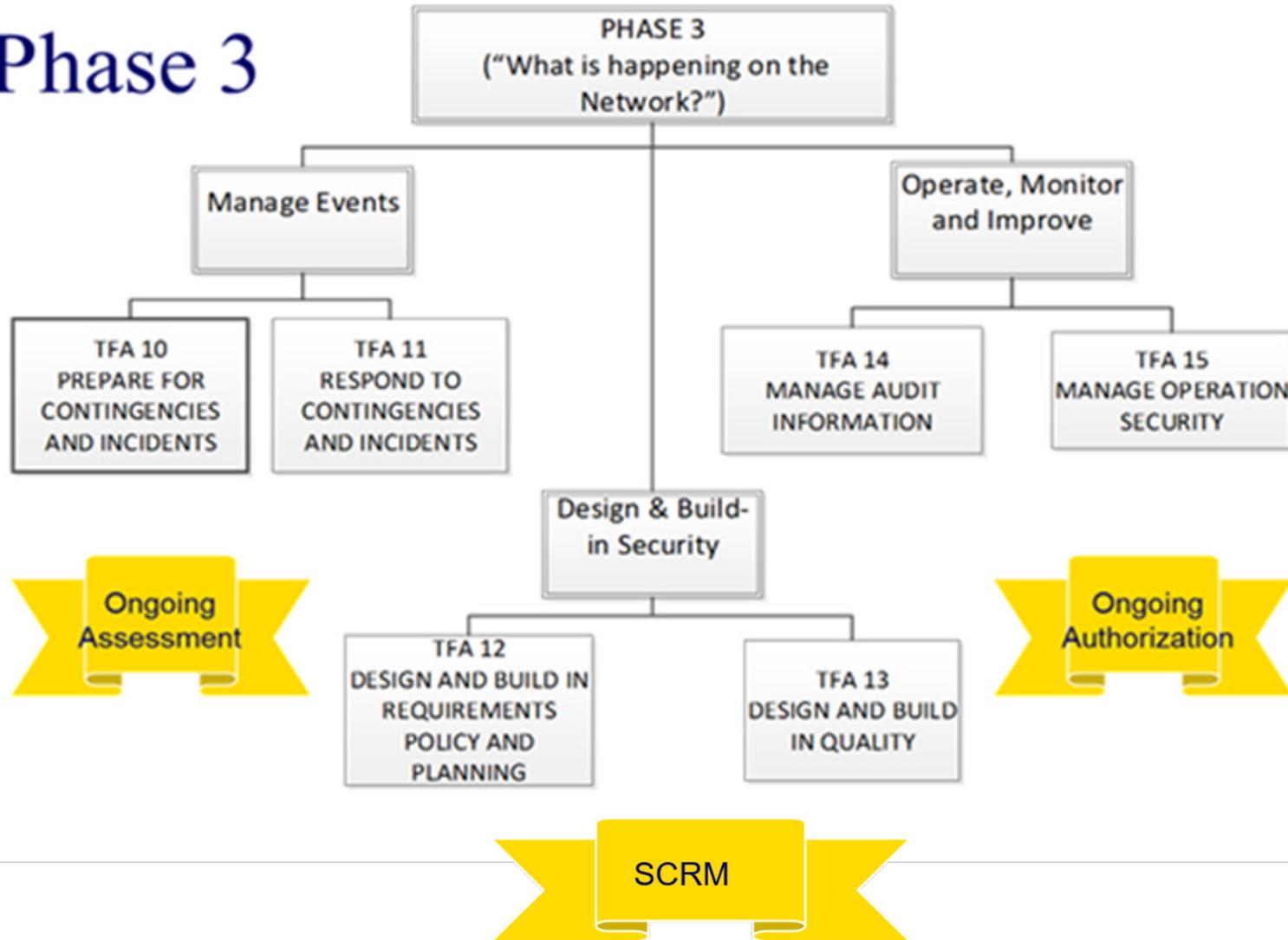


Homeland Security

Completing Requirements



Phase 3



Beyond Phase 3 Considerations

Microsegmentation

Digital Rights Management

Advanced Data Protections

Mobility Threat Protections



**Homeland
Security**

Beyond Task Order 2 Approach

Acquisition activities be considered within three categories:

- **Universal** : A given activity will apply to all agencies
- **Targeted**: Focused effort where the participants must conform to defined criteria usually related to readiness (or maturity). Agency or sub-Agency participation is independent of any groupings.
- **Selected**: Is a hybrid approach that is applied to some subset of agencies that is less than the population represented by universal, but not as limited as targeted.



**Homeland
Security**

Functional Delivery Packages

Dashboard Centric

Phase 1 and 2 excluded scopes (Cloud, Mobile, etc.)

Phase 3

1. Boundary Filtering Network (IP) based
2. Boundary Filtering Content based [Web, email, etc.]
3. Boundary Filtering Data Leak/Loss Prevention
4. BOUND-E Crypto enhancements
5. Inclusion of Incident Response
6. Inclusion of Contingency Planning and Backup/Restore
7. Incorporation of Ongoing Assessment
8. Incorporation of Ongoing Authorization
9. Incorporation of Design/Build-in Security (SW Assurance)



**Homeland
Security**



Homeland Security

Information on CMaaS BPA :

CDM@GSA.GOV

Queries on CDM Program:

CDM.FNR@HQ.DHS.GOV

My Contact:

Jim.Quinn@HQ.DHS.GOV



**Homeland
Security**

Questions and Answers

What is the impact of ...??

What about??

How did the stakeholders adjust to??

What would you do differently about??

What should I do about??

What would you recommend for??

How much time did it take to??

How are you maintaining 95% compliance with VUL CAP....??

How did you handle ... (latency, centralization, control issues, etc.) ??



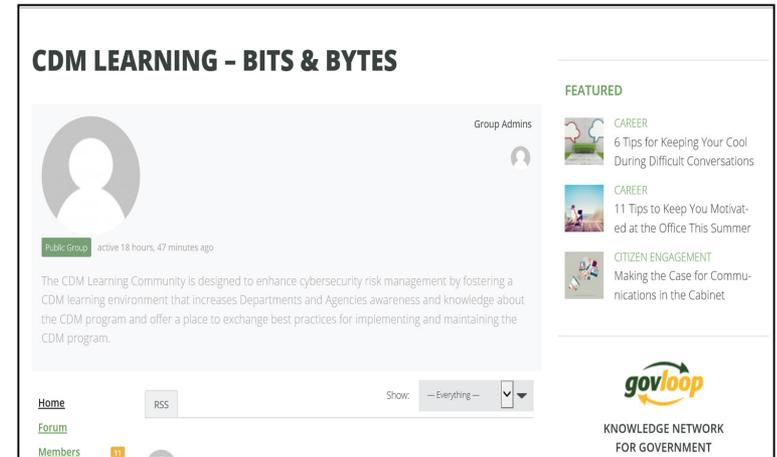
The CDM Learning Program

CDM Learning Program

- ▶ Monthly Learning Community Event (CDM-LCE)
- ▶ Monthly Webinars
- ▶ Weekly CDM Bits & Bytes
- ▶ Online Vignettes

Resources Available:

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



Sign up for the CDM learning blog:
<https://www.govloop.com/groups/cdm-learning-bits-bytes>

Sign up to receive event information:
cdmlearning@hq.dhs.gov



Event Conclusion

Thank you for attending today's CDM Webinar!

- ▶ A certificate of attendance will be available to download on the CDM Learning Program website at www.us-cert.gov/cdm/training, within one week of today's event
- ▶ Visit our website to learn more about the CDM Learning Program and upcoming events at www.us-cert.gov/cdm
- ▶ For any questions, comments, or suggestions for future topics, please email us at cdmlearning@hq.dhs.gov

