Department of Homeland Security (DHS)
Continuous Diagnostics & Mitigation (CDM)

CDM Program Briefing

What is CDM?

- The CDM program is a dynamic implementation approach to fortifying the cybersecurity of computer networks and systems.
- The CDM Program provides capabilities and tools that enable network administrators to know the state of their respective networks at any given time, by identifying and ranking problems for priority resolution. Continually monitoring networks for flaws and anomalies will alert network managers to attacks and intrusions, thereby enabling faster responses to fix vulnerabilities that allow attacks.
- CDM's intent parallels the national priority for hardening network defenses.
- CDM offers commercial off-the-shelf (COTS) tools, with robust terms for technical modernization as threats change.
- The CDM Program helps protect government IT networks from cybersecurity threats and enhances risk-based decision-making.

CDM Concept of Operations

- **Funding/Procurement Expectations**
  - Address .gov agency continuous monitoring gaps
  - Develop federal/agency dashboards
  - Strategic sourcing
- **Objective:** Harden federal networks in face of attacks
- **Scope:**
  - Unclassified .gov systems with FY 2013 funds
  - Open contract to other federal, state and local use
  - Create a federal dashboard to feed CyberScope

How CDM Works

- Agency-installed sensors that perform an automated search for known cyber flaws;
- Results feed into dashboards, which produce customized reports, alerting IT managers to their worst and most critical cyber risks based on standardized and weighted risk scores;
- Prioritized alerts, enabling agencies to efficiently allocate resources based on the severity of the risk; and
- Progress reports that track results which can be shared within agencies. Summary information can be fed into an enterprise-level dashboard to inform and prioritize cyber risk assessments.

Expected Benefits

- Achieves cost savings through tiered-price and task order discounts, enabling more efficient use of scarce resources;
- Utilizes consistent application of best practices and Commercial Off-the-Shelf (COTS) products;
- Provides near-real time results;
- Prioritizes the worst problems within minutes, versus quarterly or annually;
- Enables defenders to identify and mitigate flaws at network speed; and
- Lowers operational risk and exploitation of government IT systems and networks.

CDM– Implementation Phases

PHASE 1

- **Main Goal: Endpoint Integrity**
- Scope: Local Computing Environment (Devices)
- Areas of Focus: Hardware and Software Asset Management, Configuration Settings, Known Vulnerabilities, Malware

PHASE 2

- **Main Goal: Least Privilege and Infrastructure Integrity**
- Scope: Local Computing Environment (People), Network and Infrastructure (Devices)
- Areas of Focus: Account and Privilege Management, Configuration Settings, and Ports/Protocols/Services for Infrastructure Devices

PHASE 3

- **Main Goal: Boundary Protection and Event Management**
- Scope: Local Computing Environment (Events), Network and Infrastructure (Events), Enclave Boundary (Devices, Events)
- Areas of Focus: Audit and Event Detection/Response, Encryption, Remote Access, Access Control

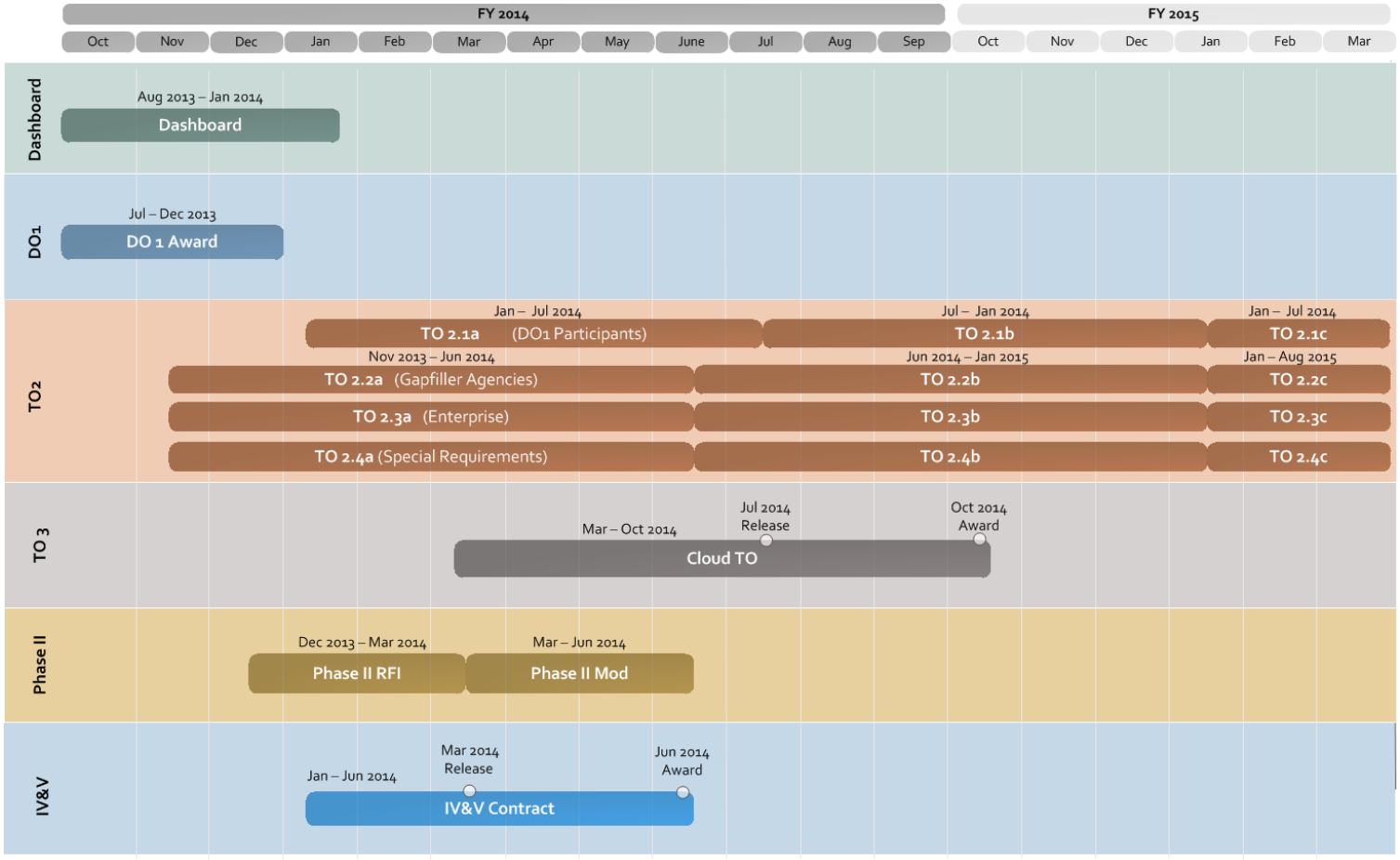
CDM Capabilities

Participation Status

- Current CDM Program Participation
  - 124 agencies have been contacted (representing 286 D/A and components)
  - 105 agencies are eligible to participate in the CDM Program and Early
  - All 23 CFO Act agencies are participating
  - Early Engagement Group is in operation

CDM Notional Task Order Schedule

Updated Dec 3, 2013



Delivery Order 1 (Commodities Only)

- RFQ released November 8, 2013
- Proposals received at GSA November 22, 2013
- Evaluations are under way
- Award will be in early 2014
- Expect to include more than 25 D/As
- Participants will be contacted to obtain delivery information (accountable property officer and instructions)
- Additional products and services to complete the CDM solution for TO 1 recipients will be from TO 2.1

Task Order 2 Approach

- Breakdown TO2 to support subgroups
  - 2.1 – Services Subgroup
  - 2.2, 2.3, 2.4 – Enterprise and Gap Filler Subgroups
- Streamline requirements where possible
- Reduce the amount of time required to setup acquisition, release the solicitation, evaluate, and make award while minimizing the likelihood of a protest.
- Identify and reduce complexities related to execution and management of each subgroup

- **Acquisition Activity – CDM is looking beyond GSA FEDSIM to assist in processing task orders under the CDM CMaaS BPA**
- **Subgroups will be iterative in the roll out of Phase I capabilities.**

Resources

CDM public website: www.us-cert.gov/cdm

CDM ordering information: www.gsa.gov/cdm

CDM Portal, Secure Community of Interest: https://connect.hsin.gov/cdm

Contact Us: cdm.fnr@hq.dhs.gov