An Enterprise Continuous Monitoring Technical Reference Model

Jointly developed by the U.S. National Security Agency, the U.S. Department of Homeland Security, and the National Institute of Standards and Technology

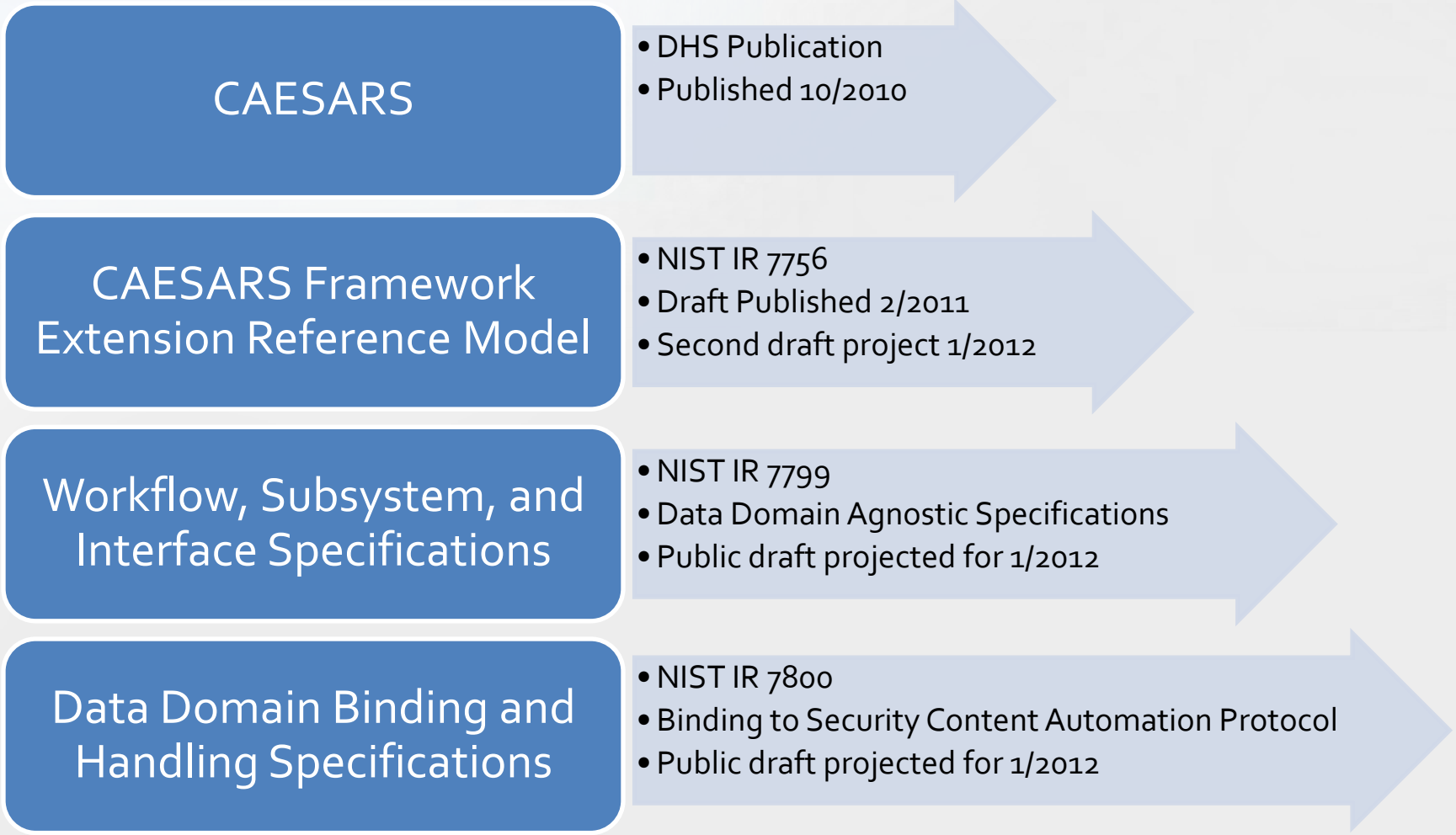
11/1/2011

Presenter: Peter Mell
Senior Computer Scientist
National Institute of Standards and Technology
http://twitter.com/petermmell

Continuous Monitoring (CM) Modeling Timeline

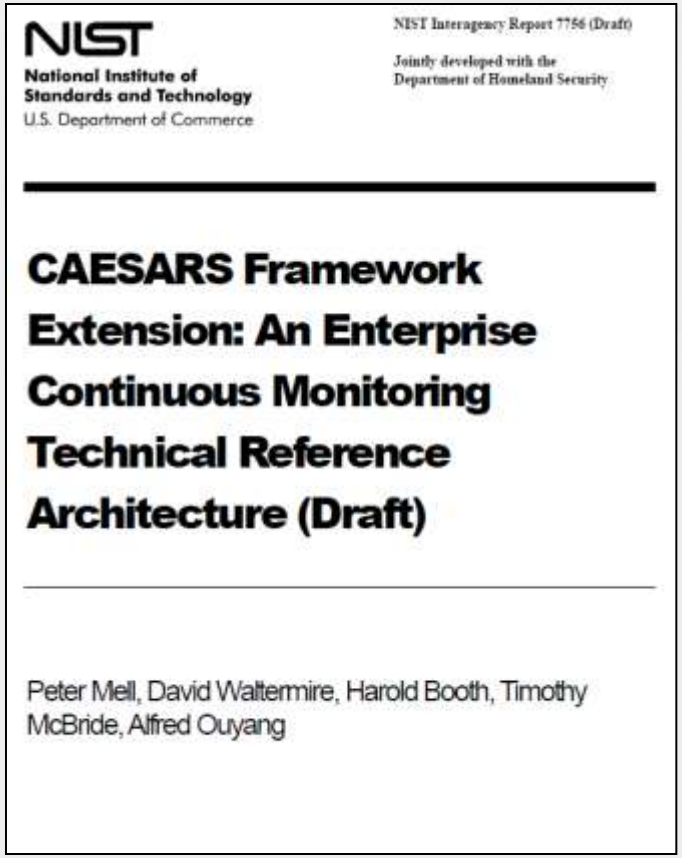
- 4/2010: Office of Management and Budget CM memo to DHS
- 9/2010: DHS published CAESARS reference architecture
  - based on Department of State, Justice, and Treasury implementations
- 9/2010: ISIMC CM initiated DHS/NSA/NIST research initiative to create the CAESARS Framework Extension (FE)
  - make applicable to entire government, adapt for large enterprises, and further leverage standards
- 2/2011: NIST and DHS published CAESARS FE (draft NIST IR 7756)
- 3/2011: CM modeling workshop at NIST March 21
- 8/2011: Initiation of weekly teleconferences on model
- 10/2011: Present draft model to the ISIMC CMWG
- 11/2011: Presentation of model at the 7th Annual IT Security Automation Conference (http://scap.nist.gov/events/index.html)
- 12/2011: Public drafts of CM specifications

CM Reference Model Documentation Architecture



CAESARS Framework Extension (FE) NIST Interagency Report 7756

- U.S. government continuous security monitoring technical reference model
- Jointly created by DHS, NSA, and NIST
- Supports the NIST SP 800-137
- Based on CAESARS: the DHS Continuous Asset Evaluation, Situational Awareness, and Risk Scoring (CAESARS) Reference Architecture
  - http://www.dhs.gov/xlibrary/assets/fns-caesars.pdf
- CAESARS FE expands on CAESARS to apply it to large enterprises and to provide enhanced capabilities



http://csrc.nist.gov/publications/drafts/nistir-7756/Draft-nistir-7756_feb2011.pdf

Continuous Monitoring (CM) Modeling Presentation Contents

- Section 1: High Level Design
  - Definitions, Characteristics, and Enterprise Architecture
- Section 2: Technical Design
  - Workflow, Interfaces, and Subsystems
- Section 3: Specification Model
  - 5 Layers of Requirements

Section 1: High Level Design

CM Model: Providing a Layered Understanding

Driving from definitions to specifications

- Definition
  - Derived Characteristics
    - Enterprise Architecture
      - Reference Model
        - Workflow
          - Subsystem Specifications
            - Interface Specifications
              - Bindings to Specific Data Domains
                - Communication Specifications

NIST SP 800-137 Definition of CM

Information security continuous monitoring is defined as maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.

This said, CM itself applies to both cybersecurity and information technology domains

Domains that CM can support

1) Vulnerability Management
2) Patch Management
3) Event Management
4) Incident Management
5) Malware Detection
6) Asset Management
7) Configuration Management
8) Network Management
9) License Management
10) Information Management
11) Software Assurance

Additional Proposed Domains:
12) Digital Policy Management
13) Advanced Persistent Threat

Source: NIST SP 800-137

Description of CM applied to Cybersecurity and for use with Technical Reference Models

Continuous security monitoring is a risk management approach to Cybersecurity that maintains an accurate picture of an organization's security risk posture, provides visibility into assets, and leverages use of automated data feeds to measure security, ensure effectiveness of security controls, and enable prioritization of remedies.

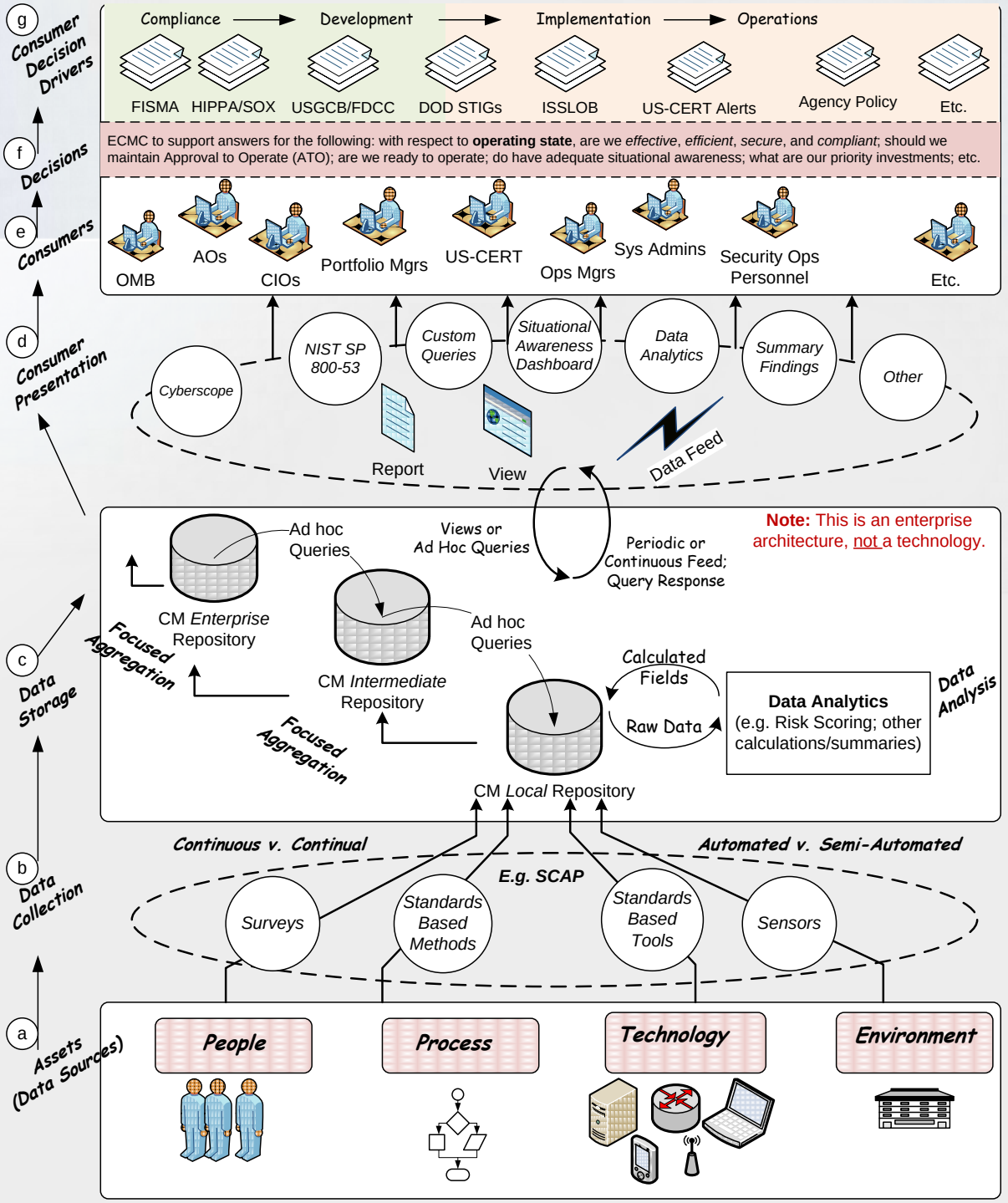
Source: NIST IR 7756

Derived CM Characteristics:

- Maintains an accurate picture of an organization's security risk posture
- Measures security posture
- Identifies deviations from expected results
- Provides visibility into assets
- Leverages automated data feeds
- Ensures continued effectiveness of security controls
- Enables prioritization of remedies
- Informs automated or human-assisted implementation of remedies

CM Enterprise Architecture

- **This shows an enterprise architecture view, not a technology focus view**

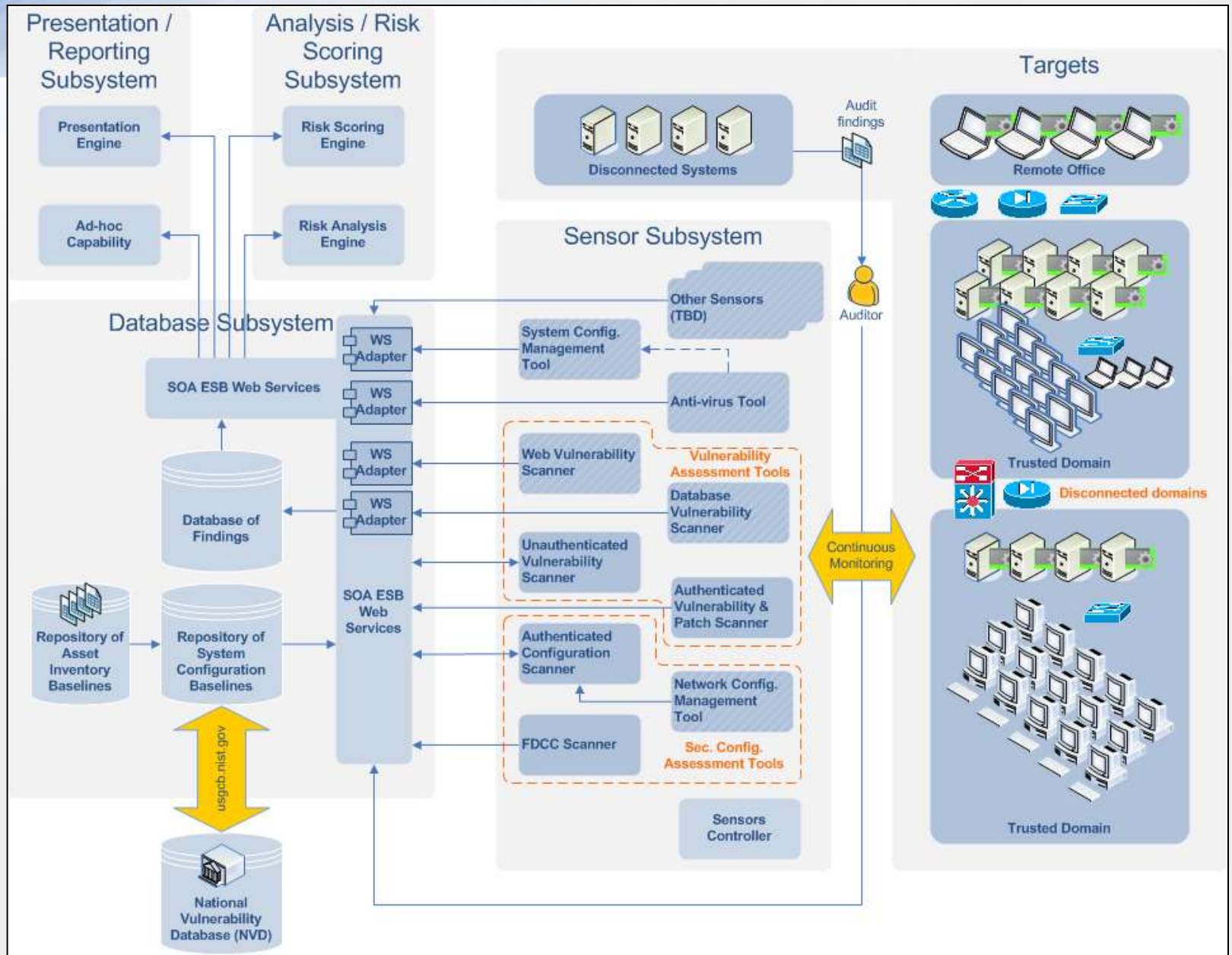


Source: NIST IR 7756
Note: Diagram derived from NSA work (original diagram credit: Keith Willett, MITRE)

Ways to Implement the CM Enterprise Architecture in Your Organization

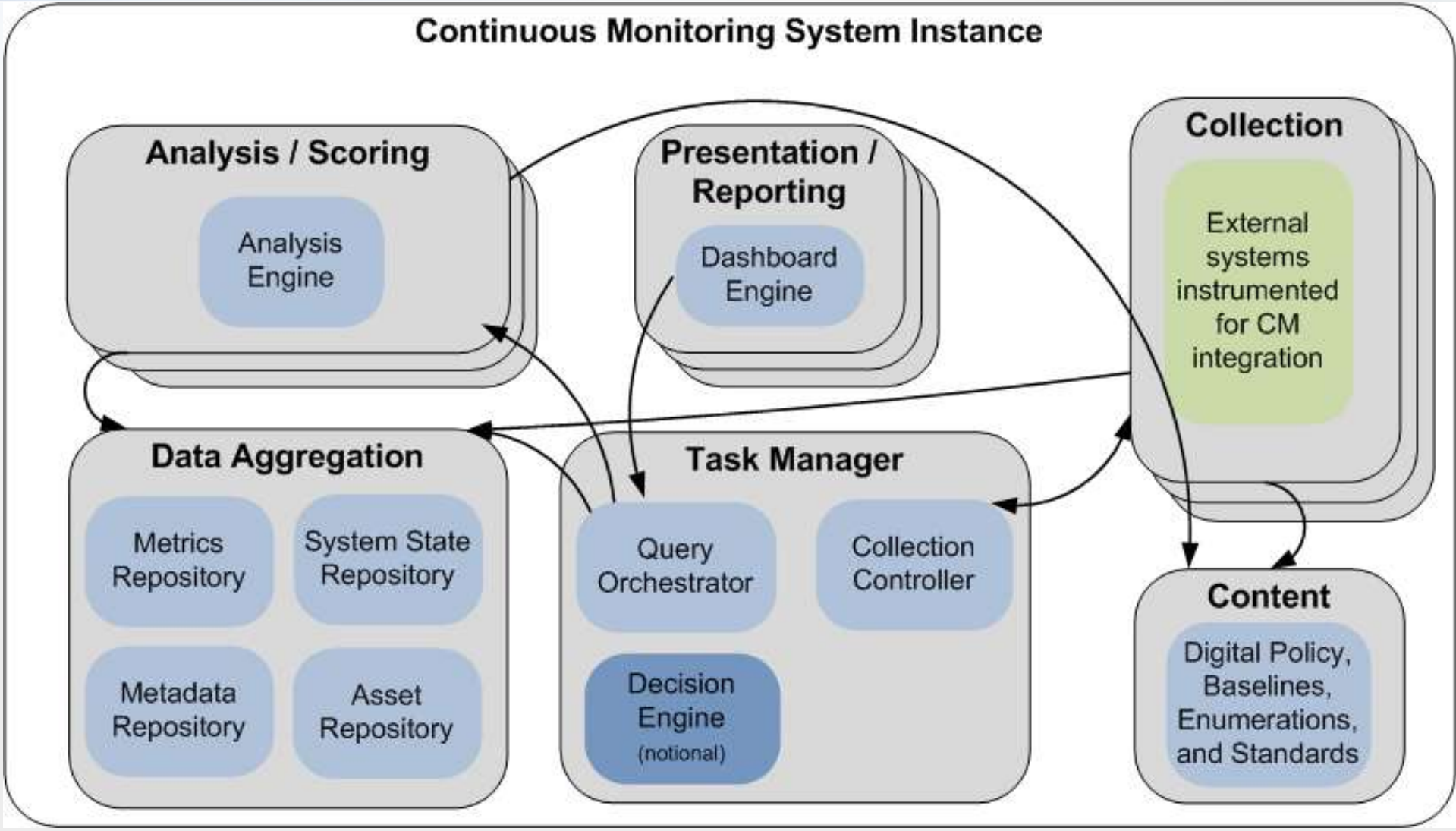
- Create ad-hoc system
  - Integrating vendor solutions to create a CM capability
  - Duplicating the work and repeating the mistakes of others
- Procure entire CM solutions from a single vendor
  - Locking into a solution that will be strong in some areas and weak in others
- Mandate a single database schema
  - Requires significant control over agency and vendor architectures
- Leverage a **CM technical reference model** and **related security standards** (e.g., SCAP)
  - Leverage your existing security products
  - Reduce integration costs
  - Combine best of breed solutions
  - Enable Federal government-wide interoperable solutions

Original DHS Continuous Asset Evaluation, Situational Awareness, and Risk Scoring (CAESARS) Reference Architecture



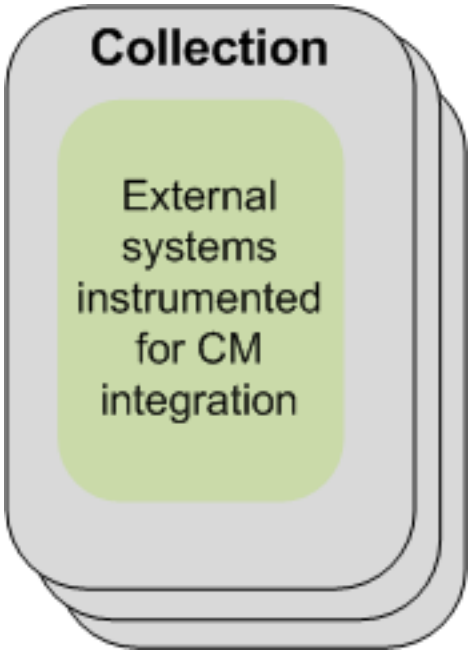
New CM Instance Model

(Organizations may have multiple CM instances)



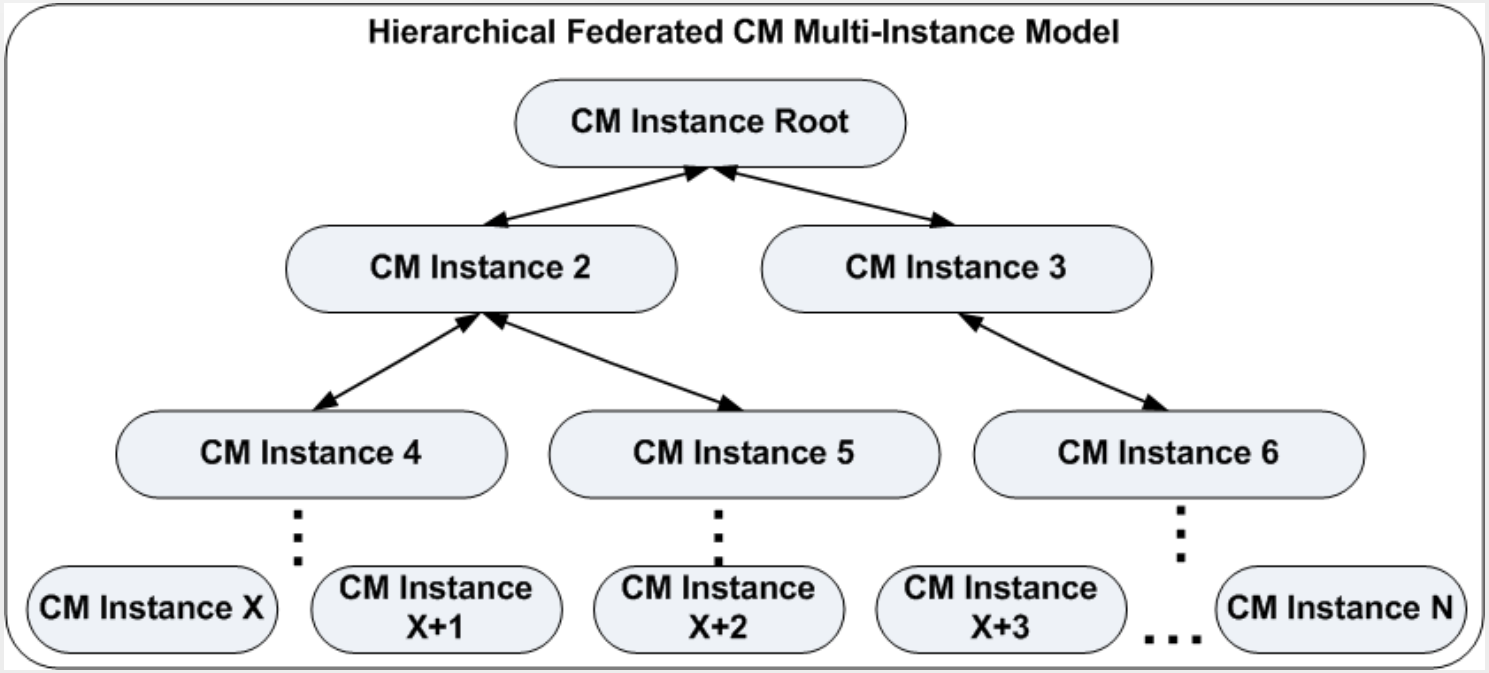
Data Collection and External System Interfaces

- CM systems must leverage (not replace) existing data collection repositories from diverse domains
- This said, existing collection systems will need to be instrumented to enable them to interface with the continuous monitoring model



Hierarchical Federated Model

- Large organizations may have more than one CM instance
- CM instances are usually arranged in a logical hierarchy
  - Aggregated reports travel up the tree
  - Data calls and configuration requirements travel down the tree
- Often CM instances have a degree of autonomy resulting in a federated style of communication
  - Each instance may have approval authority on directives from higher levels
- Lateral communication in the tree is also possible



Section 2: Technical Design

- Workflows
- Subsystem Specifications
- Interface Specifications
- Bindings to Data Domains

Technical Challenges to be Addressed by a CM Technical Reference Model

- These are areas that need to be addressed to achieve the enterprise architecture but for which commercial tools are often deficient

- Component based approach
- Creating hierarchical continuous monitoring instances
  - Inter-tier communication
  - Standardized reporting
- Dynamic, ad hoc, or operational queries
- Orchestrated control and tasking of collection systems
- Normalization of collected data
- Need to collect raw data, not results
- Ability to customize analysis and scoring based on current threats and weaknesses

CM Workflows

- Essential regardless of the CM data domains being monitored

- **WF1 Data Acquisition**: This workflow describes how raw data is collected and reported to a data aggregation repository within a single CM instance.
- **WF2 Query Fulfillment**: This workflow describes how query requests are fulfilled in both single and multi-instance CM architectures. Query fulfillment may include propagation of the query to lower level CM instances, data collection activities, and analysis of collected data.
- **WF3 Digital Policy Retrieval**: This workflow describes how digital policy and supporting content is acquired or updated from higher tier CM instances and external content repositories.
- **WF4 Digital Policy Propagation**: This workflow describes how digital policy and supporting content is propagated from a higher tier CM instance to lower tier CM instances.

Subsystem Model

- **Presentation / Reporting (1+, 3 capabilities)**
  - **User queries, dashboards, and reports**
- **Task Manager (1, 12 capabilities)**
  - **Orchestrates and tasks subsystems to support query fulfillment**
- **Collection (0+, 5 capabilities)**
  - **Collection task fulfillment**
- **Data Aggregation (1, 3 capabilities)**
  - **Central repository**
- **Analysis / Scoring (1+, 6 capabilities)**
  - **Analysis task fulfillment**
- **Content (0 or 1, 5 capabilities)**
  - **Holds digital policy and supporting content**

CM Interface Specifications

I1: Result Reporting: This interface enables reporting of data (e.g., collected raw data or analyzed query results).

I2: Content Acquisition: This interface enables the retrieval of content (digital policy and supporting data) as well as supporting the operations of insertion, modification, and deletion.

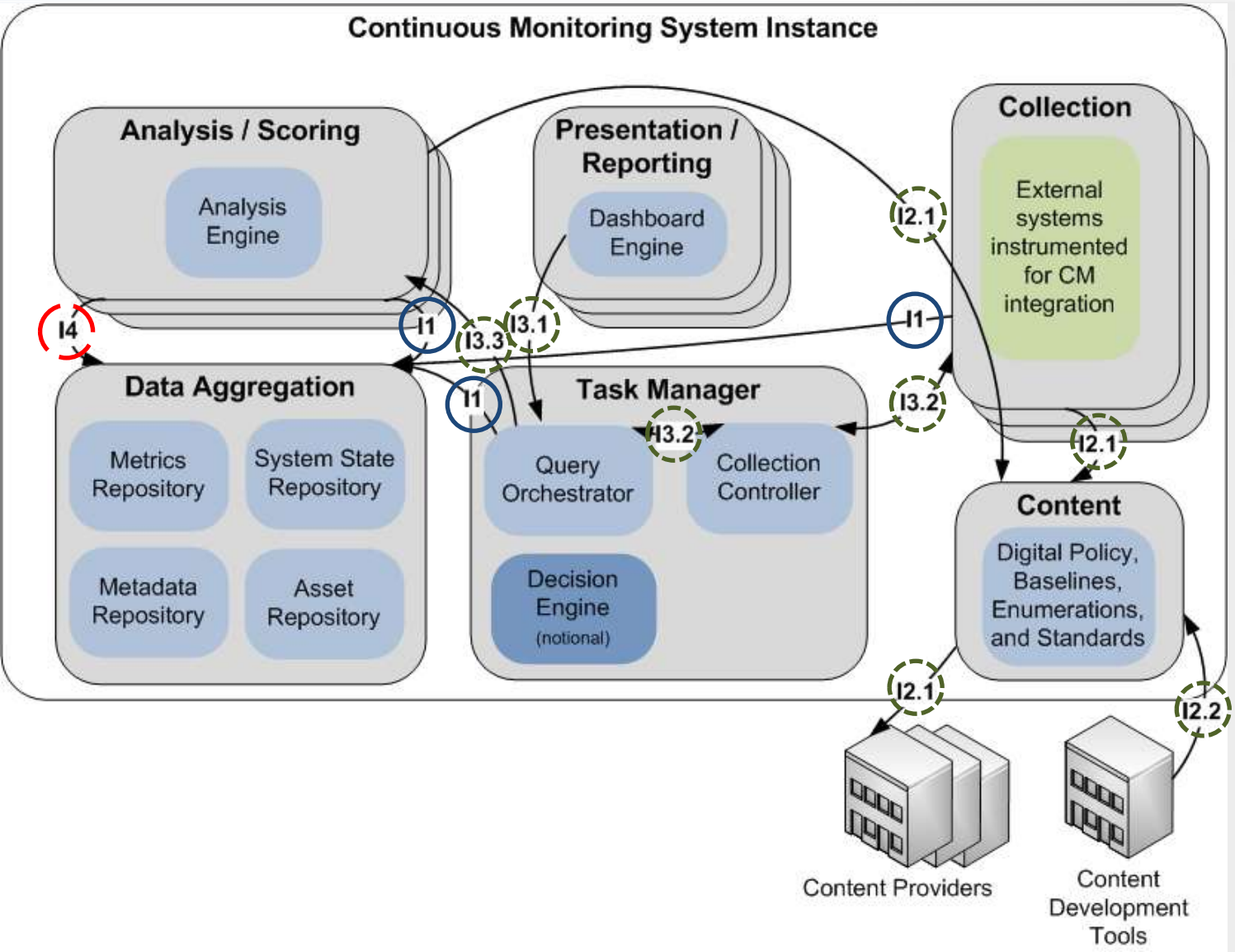
- I2.1: This interface is a subset of I2 that enables content retrieval.
- I2.2: This interface is a subset of I2 that enables the updating of content in a content repository.

I3: Querying and Tasking: This interface enables both querying and tasking between subsystems.

- I3.1: This interface is a subset of I3 that enables querying for specified results.
- I3.2: This interface is a subset of I3 that enables tasking for the collection of specific data (often used to support fulfillment of an I3.1 query).
- I3.3: This interface is a subset of I3 that enables tasking for the analysis of specific data (often used to support fulfillment of an I3.1 query).

I4: Advanced Data Retrieval: This interface enables the retrieval of data from data repositories using complex descriptors (analogous to a SQL query but without relying on database schemas).

CM Instance Model w/Interfaces



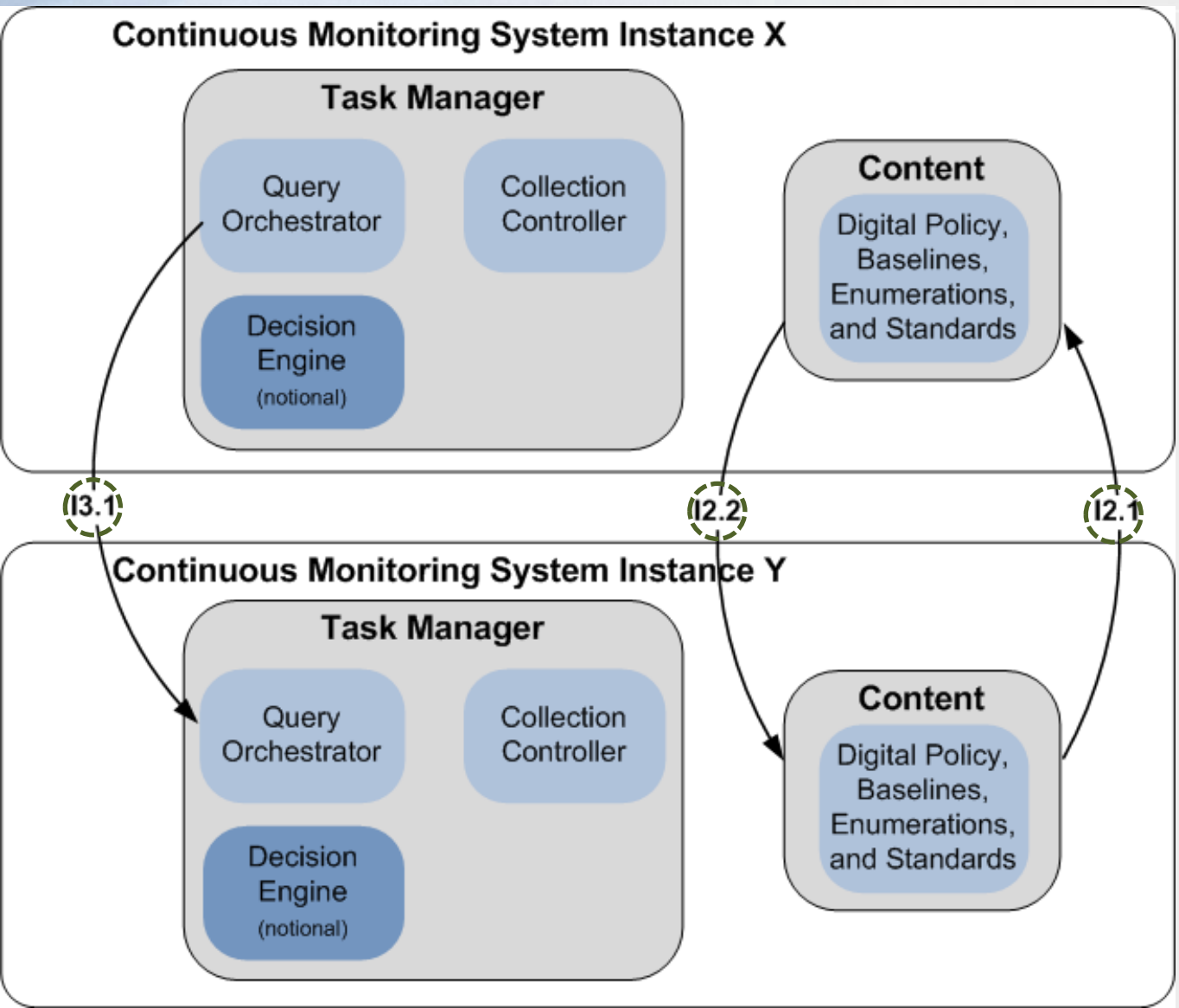
Interface Specifications:

Existing/ Standardized

Current focus/ Parameterized

Future Focus/ Proprietary

CM Multi-instance Model w/Interfaces



Interface Specifications:

Existing/ Standardized

Current focus/ Parameterized

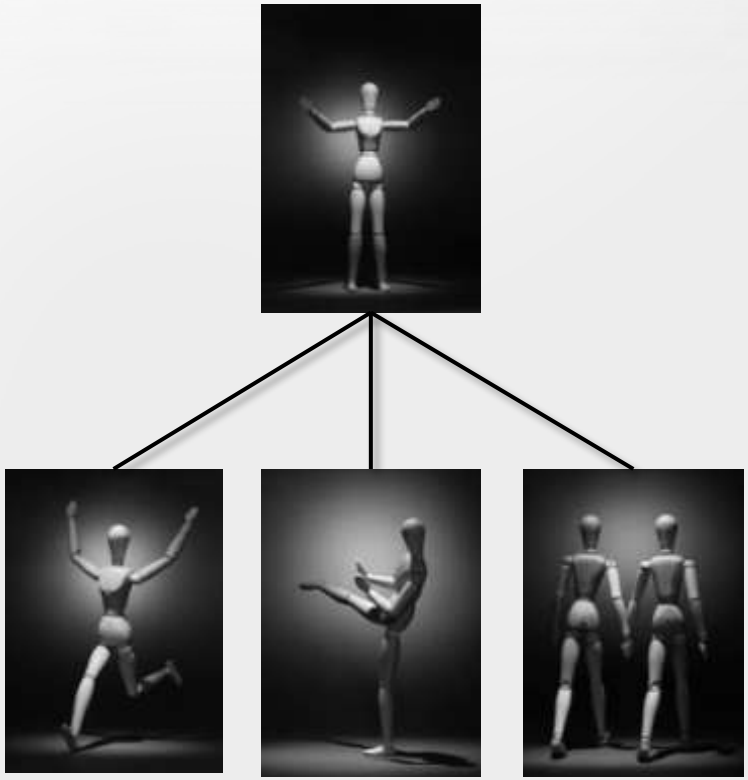
Future Focus/ Proprietary

Section 3: Specification Model

- We are NOT trying to procure a single one thing but to enable procurement of an ecosystem of tools that promote
  - interoperability,
  - hierarchical tiers,
  - federation,
  - teamwork, and
  - orchestration.

Architecture Derivations

The reference model enables derivation of specific architectures

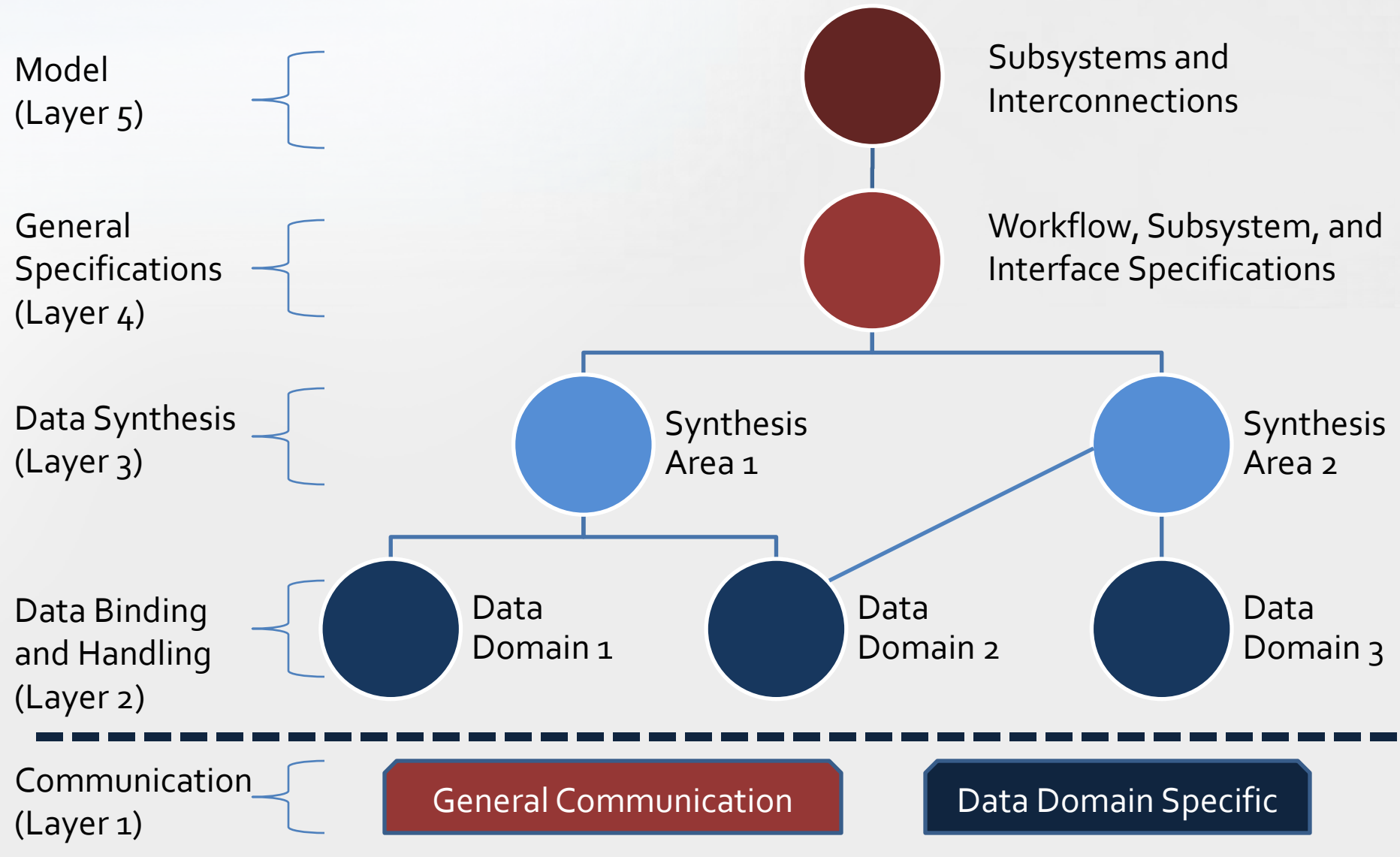


Reference Model

Derived Architectures

- Continuous monitoring domains chosen
- Specific systems and software are leveraged
- Number of instances determined

CM Specification Model



Layer 5: The CM Model

- Subsystems
  - Presentation/Reporting
  - Analysis/Scoring
  - Data Aggregation
  - Collection
  - Content
  - Task Management
- Subsystem Components
- Subsystem Interconnections
  - Describes needed communication pathways

Layer 4: General Specifications (Data Domain Agnostic)

- Workflows
  - Data Acquisition
  - Query Fulfillment
  - Digital Policy Retrieval
  - Digital Policy Propagation
- Subsystem Specifications
- Interface Specifications
  - Result Reporting Language
  - Content Acquisition Language
  - Query and Tasking Language
  - Advanced Data Retrieval Language

Layer 3: Data Synthesis (Data Domain Specific)

- Goal: Extract knowledge from the combination of multiple data domains

- Area 1: Performing multi-data domain analysis and scoring
- Area 2: Creating needed reporting views

Layer 2: Data Binding and Handling (Data Domain Specific)

- Specifications describing special handling within the model for data of a specific data domain (e.g., license management)
- Specifications for binding the high level model to data domain specific communication specifications

- Initial layer 2 specifications:
  - Asset Management (leveraging the NIST Asset Identification specification)
  - Configuration and Vulnerability Management (leveraging the Security Content Automation Protocol)

Layer 1: Communications (Covers both data domain agnostic and specific)

- These are specifications out of scope of the CM modeling work that supply a necessary foundation

- Example Foundation Data Domain Specific Specifications:
  - Security Content Automation Protocol
  - Asset Identification
- Example Foundation Data Domain Agnostic Specifications:
  - Asset Reporting Format

Remaining Work

1. Fully vet binding to asset, configuration, and vulnerability management for interoperability concerns
2. Develop a "Querying and Tasking" XML language
3. Develop a "Digital Policy Retrieval" XML language
4. Prototype the model
   - Prove out distributed communications
   - Demonstrate an implementation of novel functionality (i.e., Task Manager)
5. User configurable scoring specifications
6. Document the model in a NIST Special Publication
   - SP 800-151 reserved
   - Merge CAESARS and CAESARS Framework Extension
   - Provide guidance to agencies on usage of the model

Closing Thoughts

- We have developed a model to enable federated interoperable CM deployments
- Technical gaps remain that need to be addressed to achieve full functionality of the model
- Organizations can use the model today:
  1. Obtain high level design, workflow, and functional requirements that can guide custom CM implementation efforts.
  2. Utilize low level communication specifications together to design and develop standardized CM capabilities.
  3. Leverage the model to plan future CM design and procurements to enable federated, interoperable solutions (e.g., a government-wide capability).
  4. Influence industry to adopt specifications that enable the rapid and cost effective CM deployments (e.g., RFIs)
  5. Adopt a standardized approach to data normalization and tool integration.

Our CM Modeling Design Team

Peter Sell, Steve York
National Security Agency

Timothy McBride
Department of Homeland Security

Peter Mell, David Waltermire, Harold Booth
National Institute of Standards and Technology

Valery Feldman, Adam Halbardier,
Adam Humenansky, Zach Ragland
Booz Allen Hamilton

Alfred Ouyang, Mark Crouter
MITRE

Acknowledgements and Credit

- Much of this was inspired and encouraged by others
  - Information Security and Identity Management Committee (ISIMC) Continuous Monitoring working group
  - DHS Federal Network Security (Cyberscope and CAESARS)
  - NSA Information Assurance Directorate (IAD)
  - NIST Security Content Automation Protocol (SCAP) team
  - NIST Risk Management Framework (RMF) team
  - MITRE McLean CAESARS team
  - MITRE Bedford "Making Security Measurable" team

Summary and Questions

Presenter:

Peter Mell
NIST Senior Computer Scientist
301-975-5572
peter.mell@nist.gov
http://twitter.com/petermmell