Tasking and Targeting of Assessments

Adam Halbardier
Booz Allen Hamilton
Supporting NIST

To pass the time while you wait:

You have eight balls all of the same size. 7 of them weigh the same, and one of them weighs slightly more. How can you find the ball that is heavier by using a balance and only two weighings?

Who is contributing

- National Institute of Standards and Technology (NIST)
- Department of Defense Computer Network Defense Research and Technology (DoD CND R&T)
- MITRE Corporation

Agenda

- What is tasking?
- Why is tasking important?
- Tasking Data Model
- Recap & Conclusion

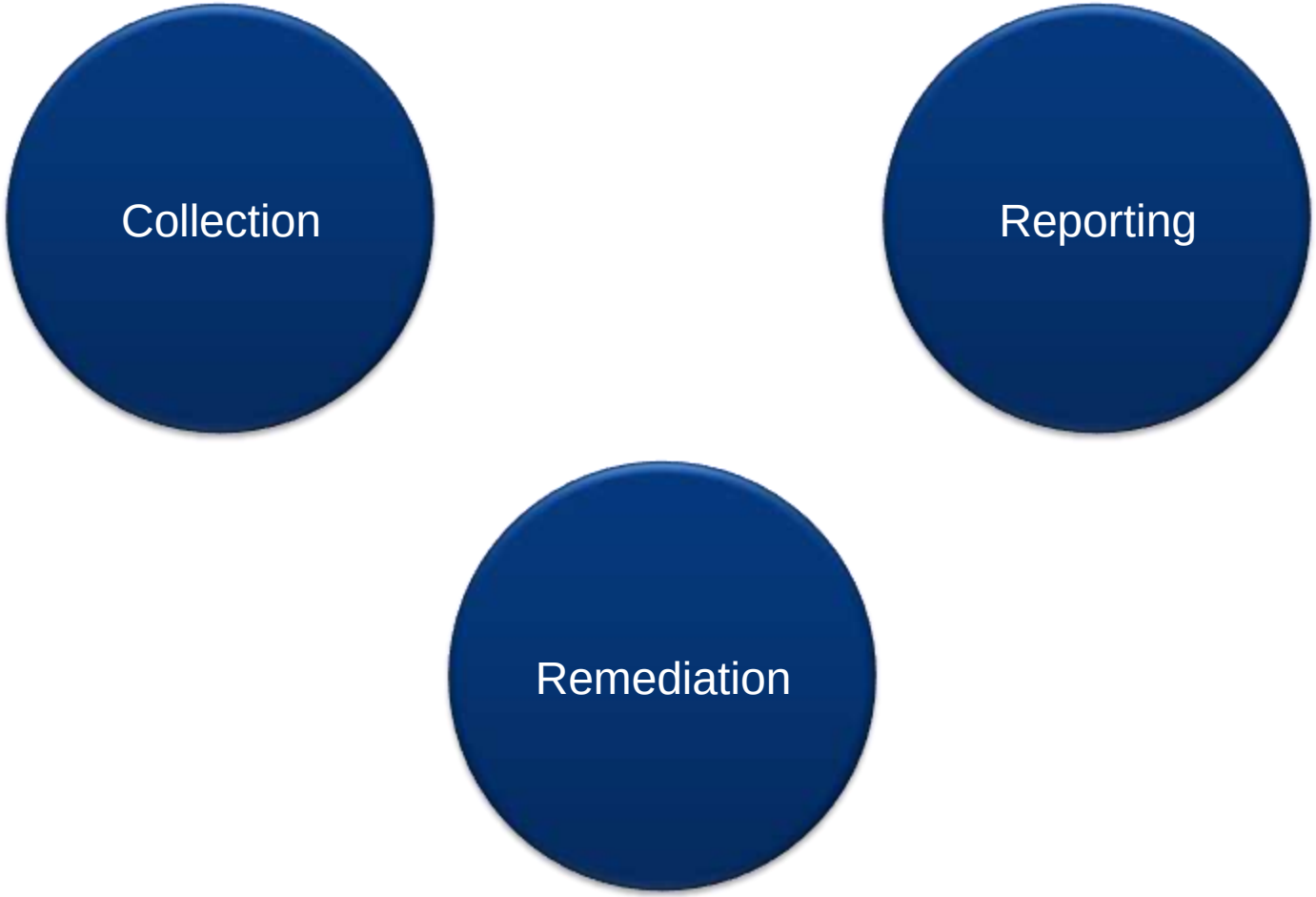
Agenda

- What is tasking?
- Why is tasking important?
- Tasking Data Model
- Recap & Conclusion

What is tasking?

Tasking is the ability to direct various components within a security automation architecture to perform some duty in a standardized manner

Types of Tasking



Types of Tasking: Collection

- To cause information to be collected
  - Configuration
  - Vulnerability
  - Asset Status/Health
  - Patch levels
  - License information
  - Inventory
- Target one or more assets

Types of Tasking: Reporting

- Both asset and summary level reporting
- Determine the required level of detail
- Target a list of assets, or a group of assets (by criteria)

Types of Tasking: Remediation

- Cause a state change on a target
  - Configuration
  - Software Management
- Target one or more assets

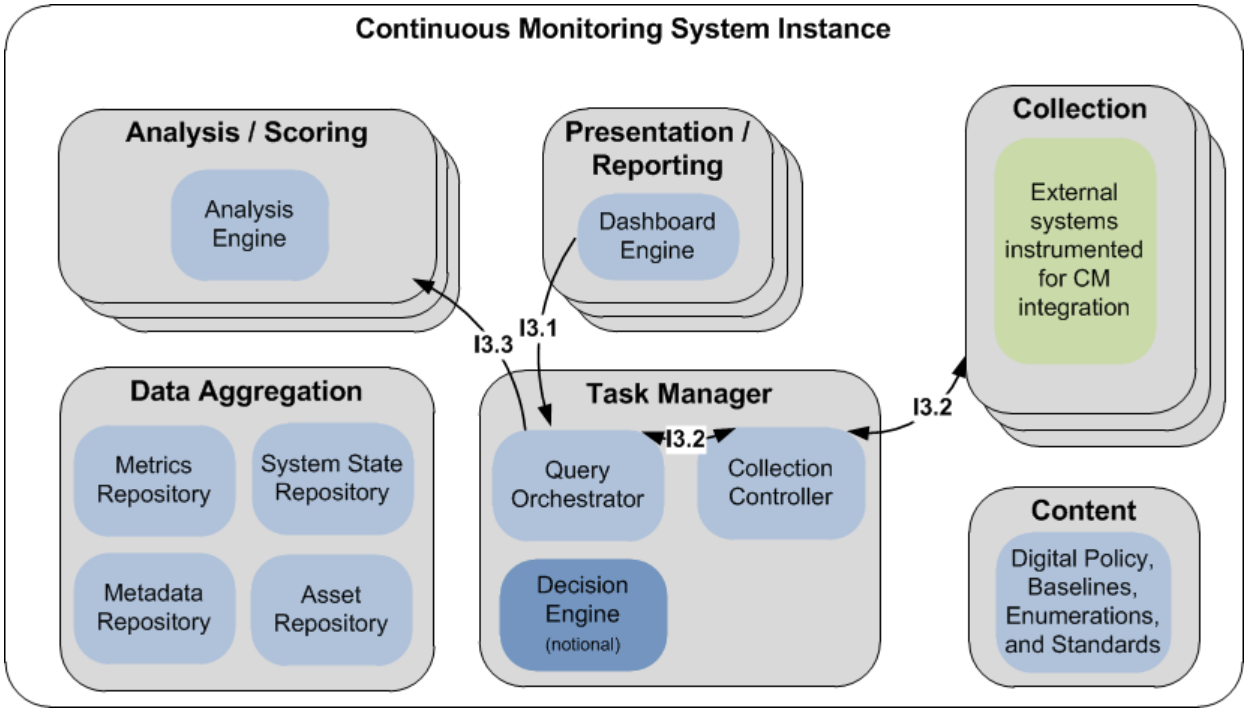
Agenda

- What is tasking?
- Why is tasking important?
- Tasking Data Model
- Recap & Conclusion

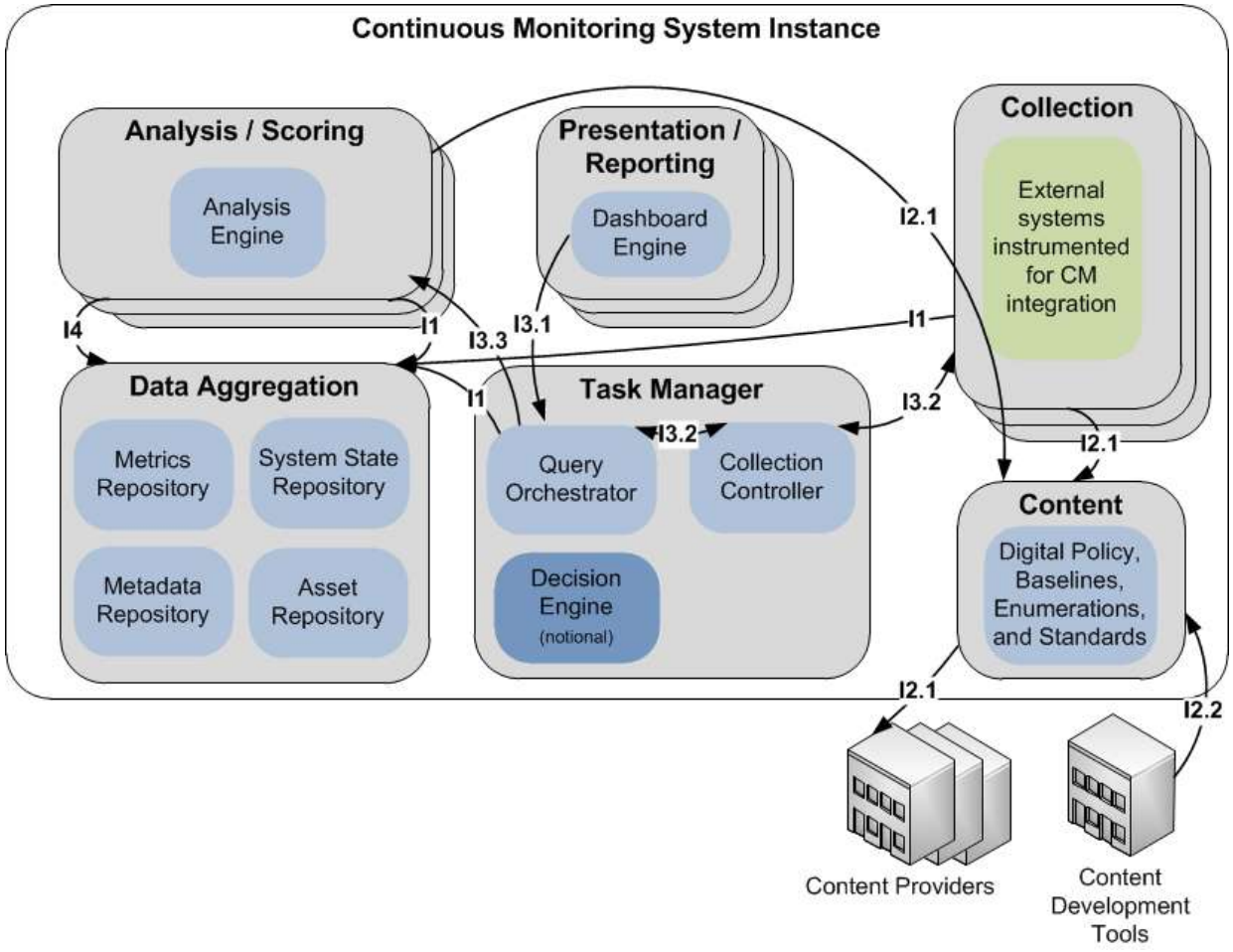
Why is tasking important?

- Tasking is necessary to orchestrate complex interactions throughout a security infrastructure
- Tasking allows dynamic, near-real-time actions to be communicated and acted upon

Example in Continuous Monitoring



Example in Continuous Monitoring



Agenda

- What is tasking?
- Why is tasking important?
- Tasking Data Model
- Recap & Conclusion

Requirements for Tasking

- Task Properties
  - Identifier
  - Traceability to source
  - Content Descriptor (embedded or pointer, metadata, parameters)
  - Target Asset Descriptor
- To be consistent with other NIST security specifications, it should be expressed in XML
- Extensible

Tasking Structure

Common Task Parameters

- Header
  - ID
  - Source Task
- Content (embedded/remote, metadata, parameters)
- Target Assets

Header

- ID
- Source Task, include (Optional):
  - Entire task, or
  - Task header

Content

- SCAP content (e.g. XCCDF, OVAL, OCIL)
- Embedded: content represented directly in task
- Remote: link to content via ID or URL
- Metadata about the content (e.g. version)
- Parameters to pass in with content on run

Target Assets

- A population description
- Select assets based on
  - List of assets using Asset Identification
  - Installed CPEs
  - FQDN Regex Match
  - Subnet

Collection Task Parameters

- Result Format (and level of detail)
- Optional: start time, end time, frequency

Result Format

- High-level format: ARF, ASR, Other
- Lower-level format as well (i.e. what to populate in ARF and at what level of detail)

Start time, end time, frequency

- Used when the task should run multiple times
- When is the first time the task should run?
- When is the last time the task should run?
- At what frequency?

Report Task Parameters

- Result Format (and level of detail)
- Data Age

Data Age

- Restrict raw data to certain age

Remediation Task Parameters

- Only common parameters

Task Results

- Indicate the status of the task
  - Success
  - Fail
  - Pending
  - Other?
- Output of Task (Optional)

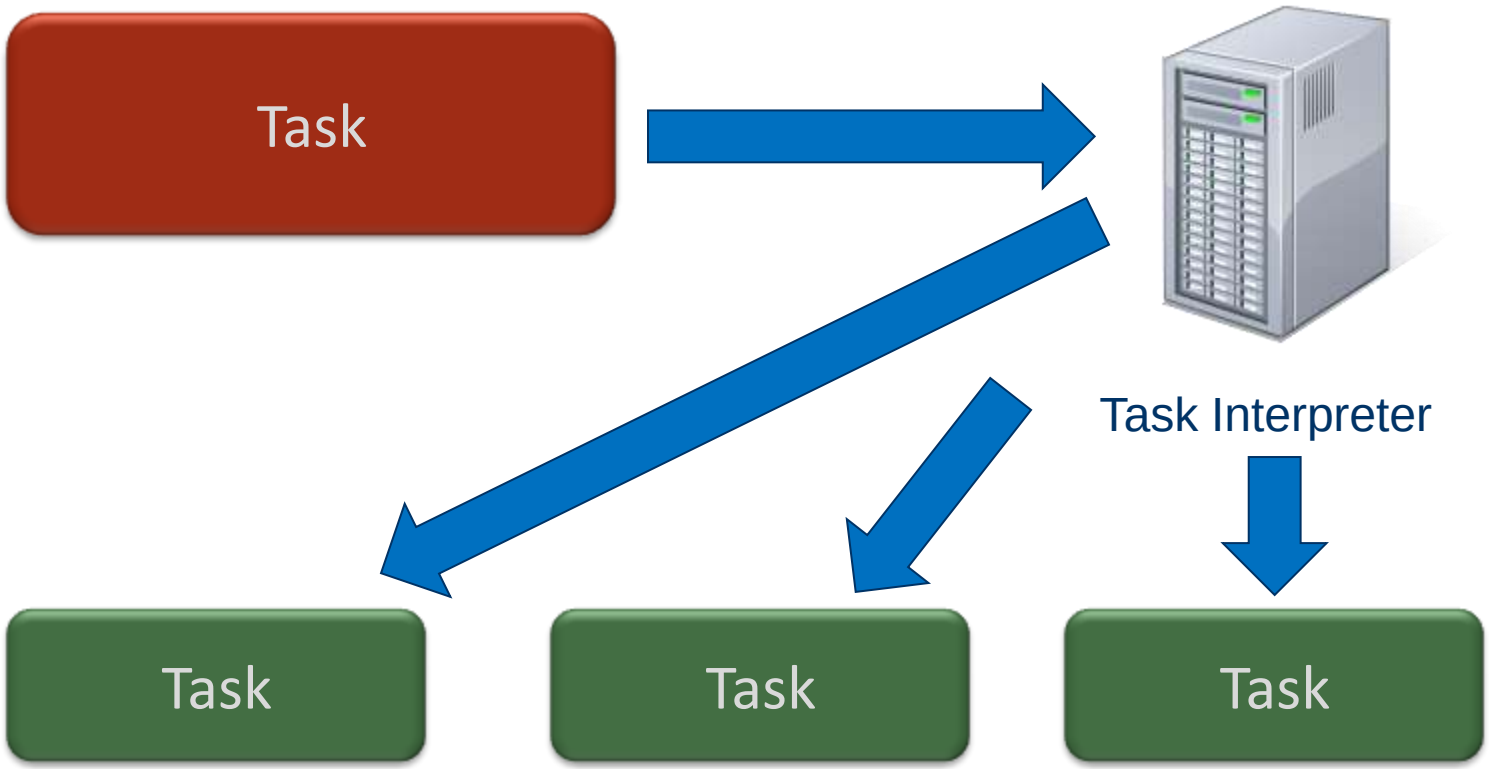
Agenda

- What is tasking?
- Why is tasking important?
- Tasking Data Model
- Recap & Conclusion

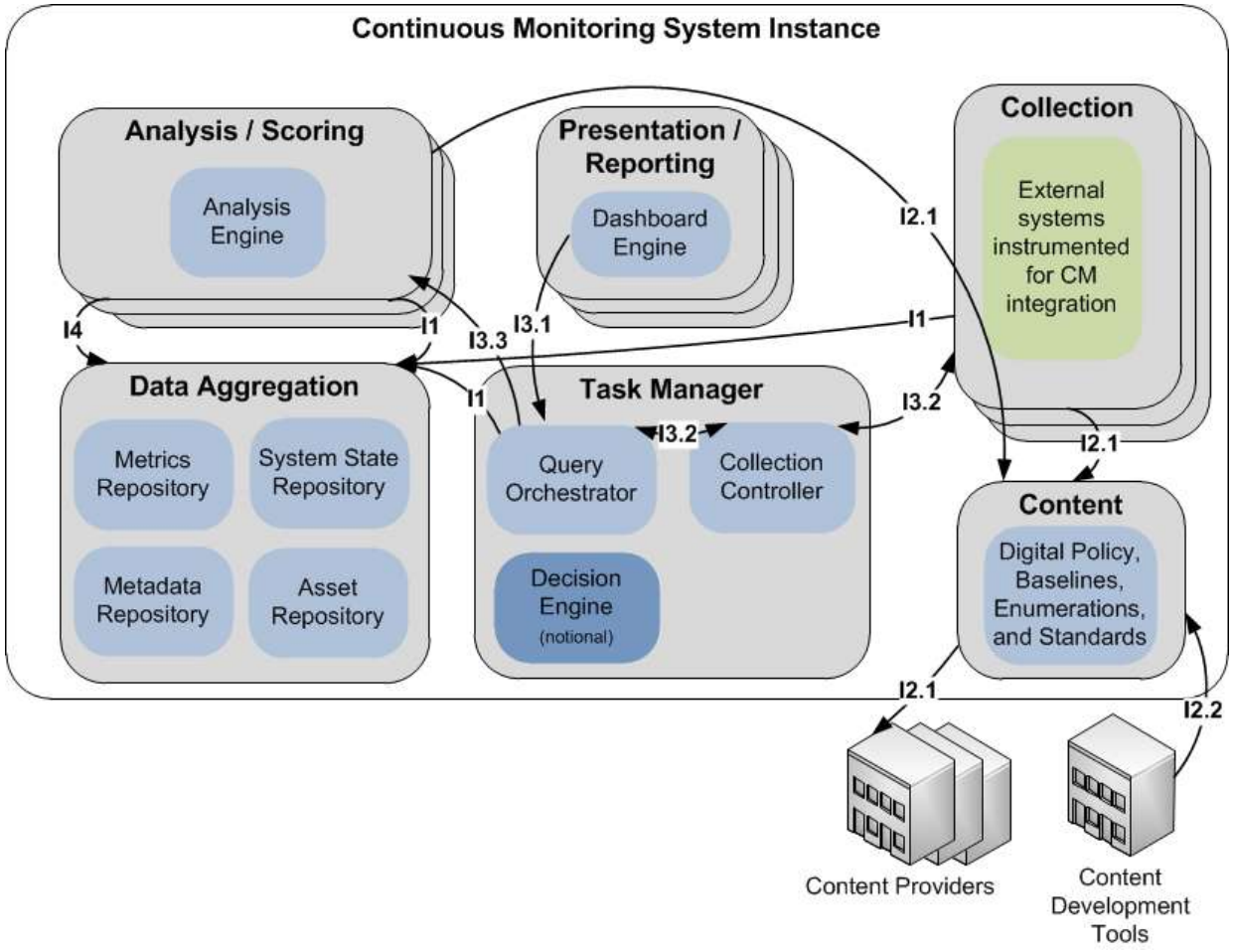
Recap

- Three types of tasks (initially):
  - Collection
  - Reporting
  - Remediation
- Enables dynamic interactions within a security automation infrastructure
- Supports task decomposition

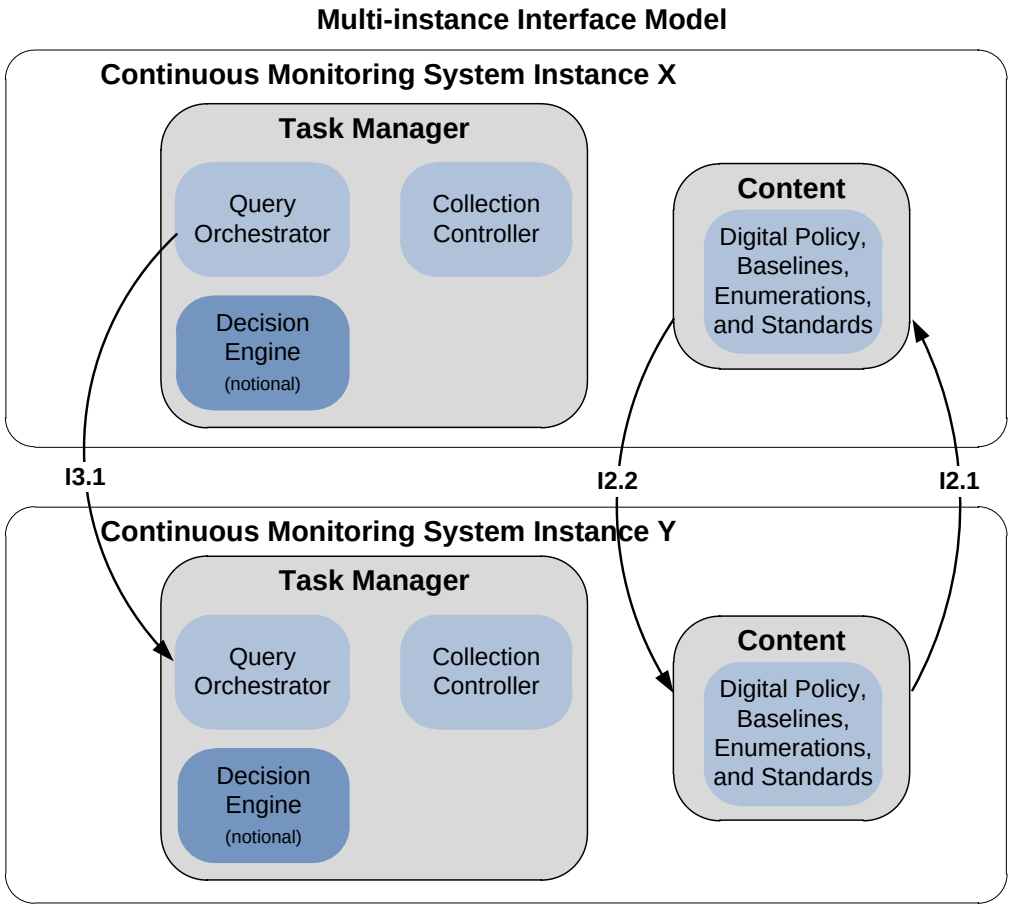
Task Decomposition



Example in Continuous Monitoring



Example in Continuous Monitoring



Status

- Tasking
  - Presenting initial design considerations
  - Open to feedback and input
- Working in Conjunction with Asset Summary Reporting
  - Currently writing NIST IR draft
  - Working out low-level data model decisions

Get Involved

- Contact any of the following people
  - Adam Halbardier – adam.halbardier@nist.gov
  - Mark Davidson - mdavidson@mitre.org
  - Dave Waltermire – david.waltermire@nist.gov
- Join the asset-dev@nist.gov mailing list (contact Dave Waltermire to be added)
- Ask about getting involved in the working group

Questions & Answers / Feedback

Adam Halbardier (Booz Allen Hamilton)
Supporting NIST
adam.halbardier@nist.gov - (310) 297-5444

Mark Davidson (MITRE Corporation)
mdavidson@mitre.org - (781) 271-3611

Dave Waltermire (NIST)
david.waltermire@nist.gov - (301) 975-3390