Goal: To have government and industry develop a consensus way forward for the endpoint posture assessment standards being developed in the IETF SACM working group.

Format: Government customers will share a set of challenges based on their requirements and the solutions that they have fielded. Vendors will provide the lessons learned supporting continuous monitoring in their products and as a service. Standards participants will describe their views on how to address the challenges. There will be time set aside to discuss these perspectives and identify how addressing these challenges could/should impact the endpoint posture assessment standards work.

General Agenda
Each day is 0900-1700. Sessions start at 0915 to allow time for administrative items or follow up items from previous day. Sessions end at 1645 to allow time for wrapping up afternoon discussions.

Day 1 Tuesday 26 August 2014 – The Context

Morning Session 0915-1230: Current Capabilities

0915-1045 Continuous Monitoring from Government Perspective – This presentation describes what we trying to achieve with current continuous monitoring activities.

- **CMRS/CDM**: Kim Watson and Joe Wolfkiel discuss the core drivers, information needs, and top issues for the two main programs [15 minutes for each speaker, 30 minutes of Q&A]
- **NVD** : NIST discusses the evolution of NVD based on the changing operational needs from consistent vulnerability identification/definition to supporting continuous monitoring of vulnerable software [15 minutes for speaker, 15 minutes of Q&A]

1045-1100 Break

1100-1230 Continuous Monitoring from Industry Perspective – This set of presentations describe what different industry sectors see as the requirements and challenges of continuous monitoring activities. [20 minutes for each speaker, 10 minutes of Q&A for each speaker]

- **Conventional Endpoints**: Kent Landfield –the need he sees from the market, the top 2 decisions we have made that have caused him problems, and his top challenge.
- **Infrastructure Endpoints**: TBD -The need they see from the market, the top 2 concerns about SACM standards for these types of endpoints, and what the top challenge is going forward.
- **Mobile Endpoints**: TBD - The need they see from the market, the top 2 concerns about SACM standards for these types of endpoints, and what the top challenge is going forward.

Afternoon Session 1330-1645: SACM and Standards Activities

1330-1400 General SACM introduction: Adam Montville – what SACM is, who is involved, what is it trying to achieve, current activities [20 minutes for speaker, 10 minutes of Q&A]

1400-1545 Other Standards Efforts [20 minutes for each speaker, 10 minutes of Q&A for each speaker, 15 minute break]

- ECP: Jessica Fitzgerald-McKay –explain what it is at a high level, what problem it is trying to solve, who is involved, top 2 points of contention

- NEA: TBD – explain what it is at a high level, what problem it is trying to solve, who is involved, top 2 points of contention
- IF-MAP/XMPP: TBD – explain what it is at a high level, what problem it is trying to solve, who is involved, top 2 points of contention, and top main lesson learned from IF-MAP.

1545-1645 Endpoints and Architecture: TBD – a quick introduction of the current SACM architecture and then discussion to highlight the key components, interactions, and areas that require more refinement. [10 minutes for speaker, 50 minutes of facilitated discussion/Q&A]

Day 2: Wednesday 27 August 2014 Software Management

Morning Session 0915-1230: Software Management Perspectives/Challenges

0915-1015 A CIOs Perspective on Software Management: TBD -what does the CIO care about with respect to software management? What are the top information needs? What are their top issues with respect to the information they currently receive? [30 minutes for the speaker, 30 minutes of Q&A]

1015-1230 Software Identification and Inventory [20 minutes for each speaker, 10 minutes of Q&A for each speaker, 15 minute break]

- **SWID Tags: Objectives and Challenges**: TBD - what is a SWID (at the high level), what operational challenges SWID Tags intended to address, and the top 3 points of contention/issues that were raised during the development/vetting process.
- **Lifecycle of SWID on MS platform**: TBD – what entity provides what information and when to create and report a SWID.
- **Lifecycle of SWID on Linux**: Steve Grubb–what entity provides what information and when to create and report a SWID
- **Data Repository and its Interface**: Brant Cheikes– critical nature (and concerns) of storing inventory information in a repository to allow singular collection to be used by the myriad of processes that care about it, e.g., vulnerability management, configuration management, license management.

Afternoon Working Session 1330-1645

Identification of the core issues from multiple perspectives and discussion to define characteristics of the solutions that address these issues. For example: What is the right level of version information that is needed for SW Inventory? How do we communicate installation footprint and/or options?

The discussion will be facilitated and multiple issues, concerns, options, etc will be discussed. This session will draw the topics from the morning session.

Day 3 Thursday 28 August 2014 - Configuration Items and Assessment

Morning Session 0915-1230: Configuration Assessment Perspectives/Challenges

0915-1045 Current Challenges with Configuration Guidance and Standards: Kim Watson, Dave Waltermire, etal - each of us describes our top 2 challenges with current standards for configuration settings (CCE, XCCDF, and OVAL) from our different perspectives. [15 minutes for each speaker, 30 minutes total of Q&A]

1045-1100 Break

1100-1130 Guidance Challenges: Greg Elin – top challenges with respect to creating, sharing, and using guidance particularly for evaluation and reporting. The previous talks tend to focus on collection guidance, but evaluation and reporting guidance are a critical part of posture assessment. [20 minutes for speaker, 10 minutes of Q&A]

1130-1230 From Lessons Learned to Possible Alternatives - The idea here is to follow some of these challenges through the Information Model and into SACM requirements. [20 minutes for each speaker, 10 minutes of Q&A per speaker]

- **Sharing the Lifecycle Burden**: Kim Watson - take the challenges related to timeliness, cost, and complexity of benchmark generation and discuss how it was split in the Information Model into platform agnostic and platform specific items. Who produces what content/guidance for platform specific posture attributes and collection/evaluation against those attributes. *Questions that need to be thought about for later in the day are: who decides "how" to collect an attribute and does that require a standard interface or schema; who decides "how" to evaluate collected attributes and what information is needed to determine that the collection is "valid" for evaluation purposes; how do we relate these items in some standardized way if different entities are authoritative for different parts?*
- **Repositories and Standards**: TBD - take the challenges related to interoperability, collaborative generation, and dynamic guidance and discuss how we need a "suite" of items to make this activity successful: standards, tools and utilities, and repositories. This talk is from the perspective of a content developer and highlights the current issues with developing standards-compliant content that can be consumed by the myriad of validated tools in diverse customer environments. It will also provide insight into using standards to interact with repositories associated with these tools. *Questions that need to be thought about for later in the day are: do we need to standardize the communication protocol, the content/data, or both for SACM repositories; are there different concerns for repositories containing guidance vs collected data; what is the business case for "sharing" guidance?*

Afternoon Working Session 1330-1645

Identification of the core issues from multiple perspectives and discussion to define characteristics of the solutions that address these issues. For example: What is the right "level" of information to standardize for interoperability? How do we use other management repositories to "feed" assessments? How do we use assessment results to "feed" other management repositories/processes? How can we modify the existing standards such that they meet our needs in a scalable and sustainable manner?

The discussion will be facilitated and multiple issues, concerns, options, etc will be discussed. This session will draw the topics from the morning session.