Continuous Monitoring as a Service

CONOPS and Deliverables

Presented by: Dr. George Moore
August 9, 2012

Homeland Security

Continuous Monitoring as a Service

Common Threads

Basic Process: D/A With nothing Procurement and Deliverables

- FEDSIM Schedules-based Acquisition
  - FedRAMP-like PMO Approval
- D/A Group Task Order Competition
  - D/As participate in requirements customization.
    - Technical Evaluation Team Participation
  - Based on D/A specific proposals
  - FedRAMP-like Provisional Authorization
  - D/A Decision on ATO
- Any Task Order under a Schedules solution will be FFP or T&M/LH

Sensors (Tools)

- Each CMaaS provider will be proposing a suite of tools.
- Selecting the CMaaS provider will also select that suite of sensors.
  - Except for D/A with existing sensors. The D/A may continue to use those.
- A standard dashboard will be provided (see next presentation).
  - Except D/As with existing dashboards may continue to use those.

Three Scenarios

- Basic Process – D/A with NO
  - dashboard or
  - sensors
- Advanced Process – D/A with EXISTING
  - dashboard and/or
  - sensors
- Micro Process – Micro D/As
- What did we miss??

Buying Group CONOPS

- To reduce cost of procurement (especially testing) propose have D/As buying CMaaS and sensors through a buying group.

- Groups would be formed by D/As (with DHS coordination) voluntarily, based on the following kinds of characteristics:
  - Similarity of Business: (e.g., Law Enforcement group)
    - Advantage: Similarity of data sensitivity
    - Disadvantage: Networks may be diverse
  - Similarity of Network Structure (e.g., device types, size, complexity?)
    - Advantage: Network similarity will simplify engineering
    - Disadvantage: May have variable data sensitivity.
  - Similarity of Business and Network Structure
    - Advantage: Seems to have the best of both
    - Possible Disadvantage: Too many groups = high task order cost.

Continuous Monitoring as a Service

Basic Process

D/A Without Dashboard or Sensors

Basic Process: D/A With nothing Services to be Received

- CMaaS Roles and Responsibilities
  - Provide D/A specific lifecycle documentation to each customer D/A.
    - Meet D/A specific environmental concerns.
    - Operate on existing D/A networks.
  - Install, Operate and Maintain -- Dashboard and Sensors
    - Meet standards for completeness and timeliness.
    - Ensure non-disruption of D/A network and operations.
    - Require minimum effort on the part of D/A to support sensors and dashboard.
  - Provide Training and Mentoring to D/A on “Governance”
  - Provide selected custom reports to D/A to support decision-making.
  - SECURE D/A CM data and do NOT unsecure D/A networks.

Basic Process: D/A With nothing Services to be Received

- DHS Roles and Responsibilities
  - Funding CMaaS tools and services.
  - Coordinate a FedRAMP-Like Certification and Accreditation.
  - Report CMaaS infrastructure to CyberScope.
  - Train CMaaS contractors on Federal CM Governance Model and how to customize this.
  - Oversee CMaaS as COTR to ensure adequate performance to D/As.
    - Receive and consider D/A performance feedback
  - Provide Dashboard for use in D/As.
  - Establish Baseline Federal Scoring and Grading Rules (and assess validity across D/As)
  - Assist D/As assess priorities and readiness for CM.
  - Reduce Cyberscope manual inputs.

Basic Process: D/A With nothing
D/A Roles and Responsibilities

- D/A Roles and Responsibilities
  - Participate in DHS led Risk and Readiness Assessments.
  - Participate in a CMaaS and Tool “buying group” with similar D/As.
    - Participate in Technical Evaluation.
    - Evaluate security plan and decide whether to grant ATO for D/A.
  - Initial Set-up
    - Provide meta-data about D/A organizations to identity IT responsibilities and IT customer roles.
    - Specify additional data grouping(s) that will make results most useful to the D/A at the operational level.
    - Identify who should have access to CM data based on those roles and responsibilities.
    - Allocate appropriate staff for TBD amount of training/mentoring in governance.
    - Establish a short “governance” process plan
  - On-Going
    - Operate a CM “governance” process to use the CM data to mitigate risk fixing the worst problems first. (See next slide.)
    - Optional: Produce ad hoc reports from dashboard data to facilitate decisions.

Basic Process: D/A With nothing
Typical CM "Governance" Activities

- D/A Stakeholder Identification/Communication
- Adjusting Federal Scoring/Grading for D/A use (optional)
- No-Fault "Pilot" operation phase.
- Transition out of "No-Fault" Phase.
- D/A Level Decision Boards
  - Risk Transfers
  - New Risk Management
  - CM Issues and Coordination Team
  - Sensor Performance Measurement/Management
- LAN Manager Assistance.
  - Tiger Teams (as needed)
  - Help Desk (as needed)
- C&A Assistance
  - Assessments (as needed)
  - POA&Ms (as needed)
- Monthly CyberScope reporting effort will be significantly reduced (through automation).

Basic Process:
Federal "Governance" Activities

- D/A Stakeholder Identification/Communication
- Assessing Risk/Priorities and D/A Readiness
- Designing Federal Scoring/Grading to compare D/As
  - Ensuring Fairness and transparency
  - Ensuring Validity and Reliability
- No-Fault "Pilot" operation phase - Transition out of "No-Fault" Phase.
- Federal Level Decision Boards
  - Risk Transfers
  - New Risk Management
  - Coordination with US-CERT, NCSD, etc.
  - CM Issues and Coordination Team
  - Sensor Performance Measurement/Management
  - Dashboard Performance/Usability Issues
  - Coordination with Standards and Policy (Across domains)

Basic Process:
Federal "Governance" Activities

- D/A Manager Assistance.
  - Tiger Teams
  - Help Desk
  - User Group to Share Problems and Solution
  - Website to provide simple "How-to" Assistance
- C&A Assistance
  - Models for using CM in Assessments
  - Models for using Dashboards as POA&Ms
- Coordination with OIG/GAO to ensure program is understood and assists D/A with audit compliance
- Coordination with private sector and non-Federal government sector

Continuous Monitoring as a Service

Basic Process

D/A With Existing Dashboard and/or Sensors

Advanced Processes:
D/A with Existing Dashboard

- D/A may continue to use existing dashboard.
  - Maintains own data feeds
  - Maintains/operates dashboard
  - Dashboard expected to meet “intent” of the Federal dashboard, but need not meet all operational and functional requirements.
  - Use Federal scoring changes to adjust D/A dashboard scores, as appropriate.
  - May choose to convert to provided dashboard in the future

- CMaaS provider will feed data to the provided dashboard
  - For these purposes (among others)
    - CyberScope reporting
    - D/A visibility into their “federal” grades
    - Coordination with CERT and other analysis.
    - Receiving Federal-level grading changes based on threat trend analysis and federal/industry situational awareness.
  - D/A and CMaaS decide whether to feed data from sensors or from D/A dashboard during task order competition.
  - D/A will make data visible in an acceptable format
  - CMaaS provider may be tasked to assist in data integration.

Advanced Processes:
D/A with Existing Sensors

- D/A may continue to use existing sensors
  - Joint D/A-CMaaS plan developed during task order competition.
  - D/A will make data visible to dashboard in an acceptable format -- CMaaS provider may be tasked to assist in data integration.
  - Sensors expected to meet “intent” of the CM program sensors, but need not meet all operational and functional requirements.
  - CMaaS provider will provide missing sensors.
  - DHS/FNS will clear plan after verifying that these conditions are met.
  - D/A may choose to move to the CMaaS suite of sensors in the future if more cost-effective.

Continuous Monitoring as a Service

Micro Process
For Micro Agencies

Micro Process

- Obtain CMaaS through a micro-agency buying group (could be as many as three?)
  - Could join one or more larger D/As as well.
- Governance provided by custom designed service organization: (D/A choice)
  - Members of the group,
  - CMaaS Provider, and/or
  - Selected larger D/A group member or volunteer.

Micro Process
Micro-D/A Roles and Responsibilities

- D/A Roles and Responsibilities
  - Participate in a CMaaS and Tool “buying group” with similar D/As.
    - Participate in Technical Evaluation (optional)
    - Evaluate Security plan and decide whether to grant ATO for D/A (use FedRAMP PA)
  - Initial Set-up
    - Provide meta-data about D/A organizations to identity IT responsibilities and IT customer roles. [Minimal]
    - Specify additional data grouping(s) that will make results most useful to the D/A at the operational level. [Minimal]
    - Identify who should have access to CM data based on those roles and responsibilities. [Minimal]
    - Allocate appropriate staff for TBD amount of training/mentoring in governance. [Minimal]
    - Establish a short “governance” process plan. [Group]
  - On-Going
    - Operate a CM “governance” process to use the CM data to mitigate risk fixing the worst problems first. (See next slide.) [Group]
    - Optional: Produce ad hoc reports from dashboard data to facilitate decisions. [Minimal]

Micro Process
Typical Micro CM "Governance" Activities

- Stakeholder Identification/Communication [Minimal]
- Adjusting Federal Scoring/Grading for D/A use (optional) [Provided by Group]
- No-Fault "Pilot" operation phase. [Provided by Group]
- Transition out of "No-Fault" Phase. [Provided by Group]
- D/A Level Decision Boards [Provided by Group]
  - Risk Transfers
  - New Risk Management
  - CM Issues and Coordination Team
  - Sensor Performance Measurement/Management
- LAN Manager Assistance [Provided by Group]
  - Tiger Teams (D/A choice)
  - **Help Desk (D/A choice)**
- **C&A Assistance [Provided by Group]**
  - **Assessments (D/A choice)**
  - **POA&Ms (D/A choice)**
- **Monthly CyberScope reporting effort will be significantly reduced (through automation). [N/A as most don't report now]**