Federal Network Security

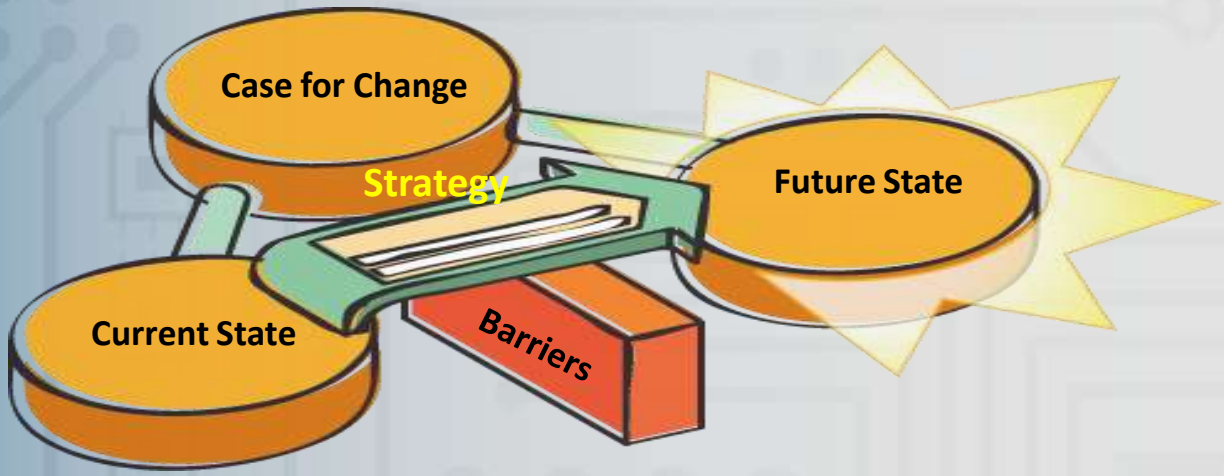
Federal Continuous Monitoring Working Group

DRAFT

March 21, 2011

DOJ Cybersecurity Conference 2/8/2011

Why Continuous Monitoring?



Current State

- Compliance Based Methods
- Historical "Point in Time" purview into agency networks
- Agency leaders & security personnel un-empowered in managing risk
- Billions spent on FISMA and C&A reporting efforts

Case For Change

- Need for a real-time purview into agency networks
- Need for Improve Risk-based decision making
- Direct positive impact on security
- Desire for higher ROI and improved mission execution

Future State

- Security Personnel & Agency Officials have real-time purview into the health of their network assets
- Ability to prioritize and remediate risk in a manner that directly improves agency cybersecurity posture

DHS Response

- Recognized the need to partner with strategic government partners to examine the feasibility of rolling out a government-wide strategy for implementation
- Examined multiple use case scenarios implemented at various federal civilian agencies
  - Scalable to large complex organizations
  - Provides a higher ROI vs. paper reports
  - Allows for enterprise-level reporting
- Published CAESARS reference architecture for continuous monitoring
- Collaborating with NIST on the CAESARS Framework Extension
- Established joint FNS/ISIMC CMWG to collaboratively develop next iteration of FISMA metrics and evolve CAESARS

CMWG Representation

- 18 Department Level Participants
- Increased Agency Component & Bureau level participation

CMWG Vision

- Promote cross-government collaboration in the establishment of a government-wide continuous monitoring and risk scoring capability.
- Focus on the technology, people and process based capabilities that will enable agencies to implement this capability at the enterprise level, and enhance the overall security posture of the United States Federal Government.

Continuous Monitoring Defined

"Continuous 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 quantify risk**, ensure effectiveness of security controls, and implement prioritized remedies."

-*NIST SP 800-137 Draft*

Goals and Objectives - Overview

- **Goal 1:** Enable Federal Agencies to implement CM/RS.
- **Goal 2:** Provide Federal Standards to allow integration of information at the Federal Level.
- **Goal 3:** Leverage Federal buying power to reduce the cost of implementing CM/RS
- **Goal 4:** Educate decision makers on the full scope of Continuous Monitoring (technology and organizational)

Continuous Monitoring Today

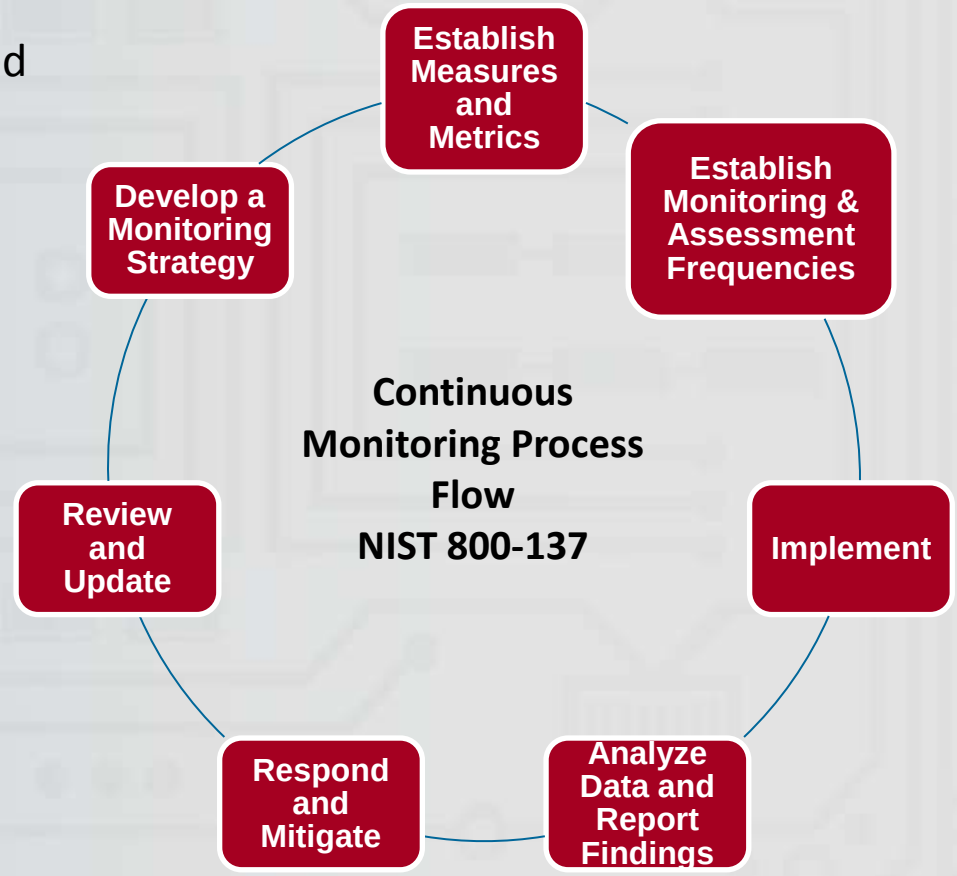
Build capability using existing data feeds and tools

- Component based approach
- Based on a standardized reference architecture
- Focused on security controls in NIST SP 800-53/CAG
- Solutions from multiple vendors can be combined together to create a CM solution

- Phase in additional capabilities in a logical manner
- Converges with capabilities found in FISMA
- FY10 Auto Feed Metrics
  - Asset Management (CPE)
  - Configuration Management (CCE)
  - Vulnerability Management (CVE)

Continuous Monitoring Evolution

- Future Capabilities
  - Expanded scope of FY10 auto feed metrics
  - Boundary Defense
  - Audit Log Analysis
  - Application Security
  - Privileges
  - Access
  - Dormant Accounts
  - Ports, Protocols, and Services
  - Data Leakage Protection
  - Others



Derived Capabilities of a CM Program

- Maintains an accurate picture of an organization's security risk posture
- Provides visibility into assets
- Leverages automated data feeds
- Allows for Quantification of risk
- Ensures continued effectiveness of security controls
- Informs automated or human-assisted implementation of remediation
- Enables prioritization of remedies
- Empowers employees at multiple levels within the organization

SAIR Tier III

- Targeting Continuous Monitoring Tools and Services
- In the planning stages
- Looking at a strategy and alternatives that would allow products to be added as they mature
- Considering a series of acquisitions
- Collaborating across all government agencies on requirements and strategy.
- Possibly releasing a RFI or Draft RFQ in Q4 2011

More information

- Continuous Monitoring Working Group

https://max.omb.gov/maxportal/register/group/EGOV.ISIMC.CMWG

- Enterprise Continuous Monitoring Capability

https://www.intelink.gov/sites/gig-ia/ECMC/default.aspx

Questions?