FISMA & Security Automation
Agenda

- Federal Network Security (FNS) Vision and Process
- Important Overview
- Visual Representation
- Simple Framework to Drive Maturity
- Notional “End-State”
- Activities
FNS Vision and Process

**VISION:** To be the recognized leader for **driving change** that enhances the **cyber security posture** of the Federal Government

Assess Enterprise Needs and Required Capabilities
- Identify and prioritize actions required to mitigate risks and improve cyber security posture across the Enterprise

Influence Policy and Strategies to Implement
- Promote actionable cyber security policies, initiatives, standards, and guidelines for implementation

Drive Implementation of Capabilities
- Enable and drive the effective implementation of cyber security risk mitigation activities and capabilities

Measure and Monitor Implementation and Security Posture
- Measure and monitor Agency implementation, compliance (with published policies, initiatives, standards, and guidelines), and security posture

Simultaneous and Iterative Process!
Important Overview

- Cyber Ecosystem is Complex – Defending our Networks and Improving Cybersecurity Posture Requires Management of ALL Ecosystem Components

- Effective Management Requires:
  - Identifying what to monitor and mitigate (SP800-53, CAG, etc…)
  - Efficient, Accurate, and Timely collection and integration of a wide range of “data feeds” (Defining Capabilities and Maturing to Full Automation)
  - Immediate mitigation actions (Prioritizing, Accountability, Empowering to Act)

- Driving this across the USG requires:
  - Collaboration (D/As, Private Sector, NIST, NSA, DHS, etc…)
  - Establishing goals and evolving goals to drive maturity (FISMA)
  - Balancing/Aligning standards development/adopton with operational needs
  - Facilitating Agency Implementation (Architectures, Contract Vehicles, etc…)
  - Minimizing Disruptions/Disconnects (IG Coordination, etc…)
  - Encouraging Vendor Adoption (COTS, Content Delivery) (Building Demand)
  - Effectively Communicating our Progress (link to goals/metrics) and Plans
Mature Enterprise-Wide Cybersecurity Capabilities

- System Inventory
- Asset Management*
- Configuration Management*
- Vulnerability Management*
- Identity and Access Management
- Data Protection
- Boundary Protection
- Incident Management
- Network Security Protocols
- Remote Access/Telework Management
- Training and Education
- Software Assurance
- Supply Chain
- Others…

*Standards Exist (SCAP)–Continue Focus on Content

- Equates to Complex Business Process Improvement Projects
Simple Framework to Drive Maturity

• Given the complexity of this process improvement effort, we have to (and already are in the FY10 FISMA metrics where possible) track 3 different levels of metrics

• Levels of Maturity
  • **Implementation** Levels (Manual Reporting)
    • To what degree is the capability implemented?
  • **Effectiveness/Quality** Levels (Partially Automated Reporting)
    • To what degree are the desired outcomes being measured and managed?
  • **Impact** Levels (Automated Reporting)
    • To what degree is risk being reduced?

• Examples:
  • **Implementation:** 40% of Agency XYZ’s IT assets are covered by an automated capability providing visibility at the Agency level into detailed configuration information
  • **Effectiveness/Quality:** For assets covered by an automated configuration management capability, Department of X can aggregate that information in 5 days
  • **Impact:** Agency XYZ has the following types and numbers of configuration deviations:
    • CCE #ABC: 290; CCE #XXY: 89; etc…
Highly automated, effective capabilities enabling timely and efficient mitigation activities with the greatest impact - FISMA Reporting is a by-product!
Activities

• FY10 Annual FISMA Reporting requires auto feeds for three SCAP-based data sets (auto-feeds into CyberScope)
  • FY11 FISMA Reporting seeks to expand the number of auto-feeds

• Published initial CyberScope Schema for FY10 auto-feeds

• Published a Continuous Monitoring Reference Architecture (CAESARS) on 9/1/10

• Established SAIR TIER I BPA with GSA in June 2009 based on SCAP Validated Tools
  • McAfee, Gideon Technologies (now Symantec), BIGFIX (now IBM)

• Defining requirements for SAIR TIER III (continuous monitoring) BPA to expand the number and types of vendors available to Agencies

• Considering the development of a USG approved product list based on SCAP
Activities (2)

- NSA/NIST/DHS co-sponsored **Vendor Outreach** effort in Mountain View, CA on 8/13/10
  - 120+ participants

- Established a joint **FNS/ISIMC Continuous Monitoring Working Group (CMWG)** 8/15/10
  - Group will drive definition of additional “data feeds” (to be used for FY11 FISMA Reporting)

- Conducting joint **FNS/NIST CM Workshop** as part of ITSAC Conference on 9/29/10 to engage vendor community
  - CMWG members will facilitate small groups with vendors to define additional “ecosystem” data feeds

- Conducting joint **NCSD/ISIMC Conference** on 10/19-21
  - Continuous Monitoring Sessions