Homeland Security

Federal Network Security Initiatives

AN OVERVIEW BY MATT COOSE

Agenda

- **The FNS Mission**
- **Authorities and Approach**
- **Organization**
- **Security Automation Initiatives**
  - FISMA & CyberScope
  - Strategic Sourcing
  - Reference Architectures
  - Next Generation

Mission: *Drive change that enhances the cyber security posture of the Federal Government*

AS-IS

- Inconsistent understanding of network topology
- Subjective measures of cybersecurity posture
- No centrally defined and communicated cyber security baseline
- Numerous and overlapping “audit” bodies (IG, GAO, etc)
- Funding and authority of CIOs is variable across D/As

TO-BE

- Fully mapped and understood network topology
- Objective quantification of cyber security posture
- Established, communicated, and continuously improving cyber security baseline
- Coordinated/aligned audit assurance responsibilities
- Sufficient and consistent funding and authority for D/A CIOs

Authorities

The FNS mission areas were derived from the following statutory requirements and policy:

- **Federal Information Security Management Act 44 U.S.C § 3546 (FISMA)**
- **Homeland Security Act of 2002, Public Law 107-296 (HSA2002)**
- **Homeland Security Presidential Directive 23 (HSPD23)**
- **Homeland Security Presidential Directive 7 (HSPD7)**
- **Critical Infrastructure Identification, Prioritization, and Protection, December 17, 2003 (CIIPP)**
- **National Strategy to Secure Cyberspace, February 2003 (NSSC)**
- **Comprehensive National Cybersecurity Initiative, 2008 (CNCI)**
- **OMB Memorandum: M-08-05, Implementation of Trusted Internet Connections, November 20, 2007 (TIC)**
- **OMB ISSLOB designation letter dated 06/06 (ISSLOB)**
- **OMB Memorandum: M-10-15, FY2010 FISMA Reporting Instructions, April 21, 2010 (FISMA)**
- **OMB Memorandum: M-10-28, Clarification of EOP/DHS Cybersecurity Responsibilities, July 6, 2010 (FISMA)**

FNS Process

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

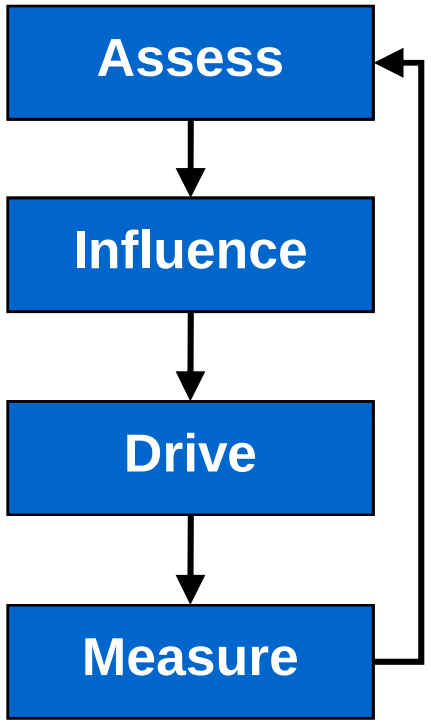
- **Promote actionable cyber security policies, initiatives, standards, and guidelines for implementation**

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!

Homeland Security

General Approach to Security Automation

- **Cyber Ecosystem is Complex – Improving Posture Requires Management of ALL Ecosystem Components**

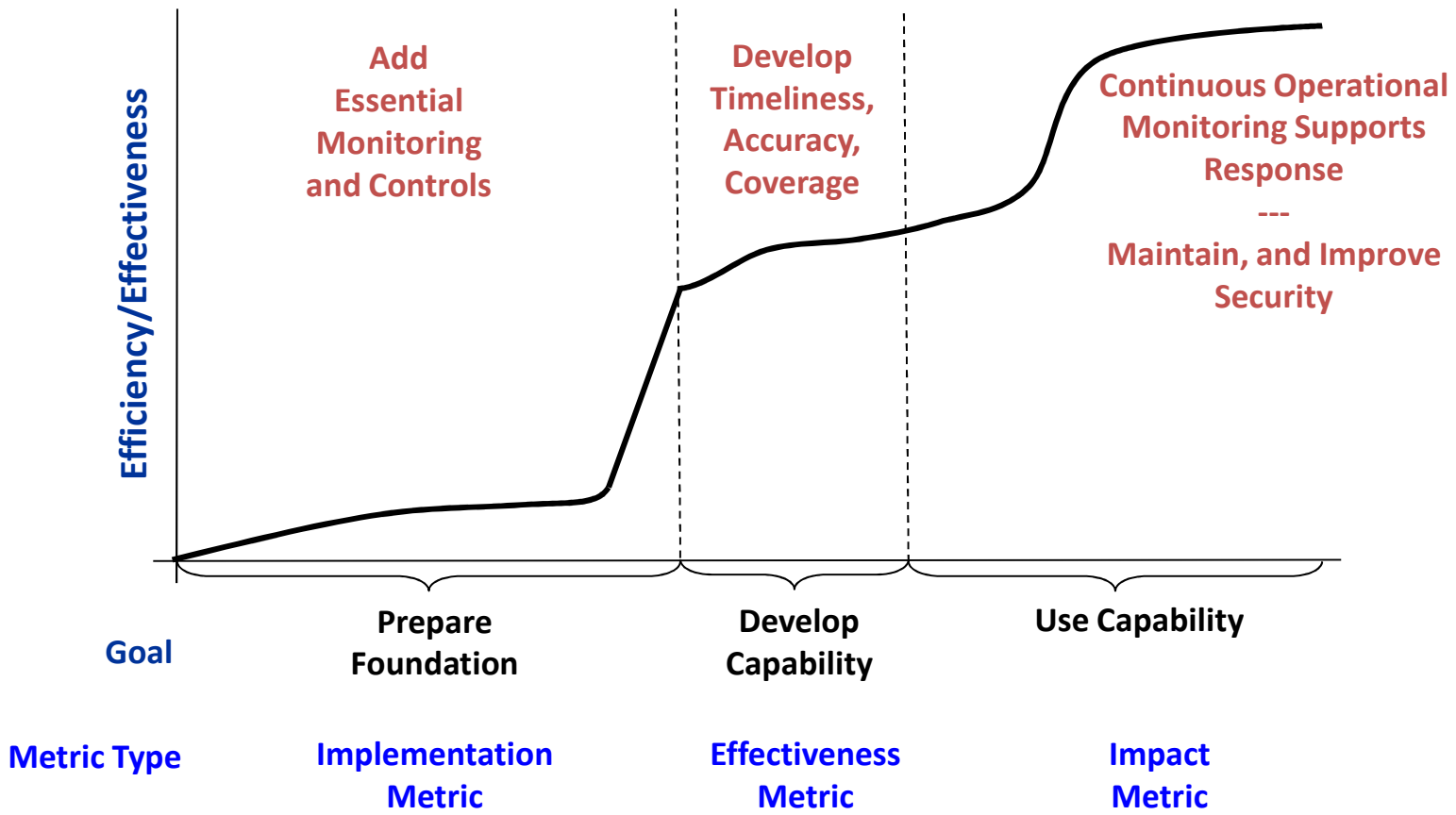
- **Effective Management Requires (OODA Loop):**
  - Identifying what to monitor and mitigate (SP800-53/CAG, Ecosystem Components…)
  - Efficient, Accurate, and Timely collection and integration of a wide range of "data feeds" (Defining Capabilities and Maturing to Full Automation)
  - Immediate mitigation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

Path to Real Impact Through Automation

- **3 Levels of Metrics/Maturity**
  - Implementation Levels (Manual Reporting)
    - To what degree is the automated 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, Agency XYZ can aggregate that information in 5 days
  - **Impact:** Agency XYZ has the following types and numbers of configuration deviations:
    - CCE #234: 290; CCE #378: 89; etc…

Capability Maturity – Another View



Homeland Security

FISMA Automation Focus Today

- **FY10 Auto Feed Metrics**
  - Asset Management (CPE)
  - Configuration Management (CCE)
  - Vulnerability Management (CVE)

ISSLOB Products & Services

Multi-Faceted Approach:

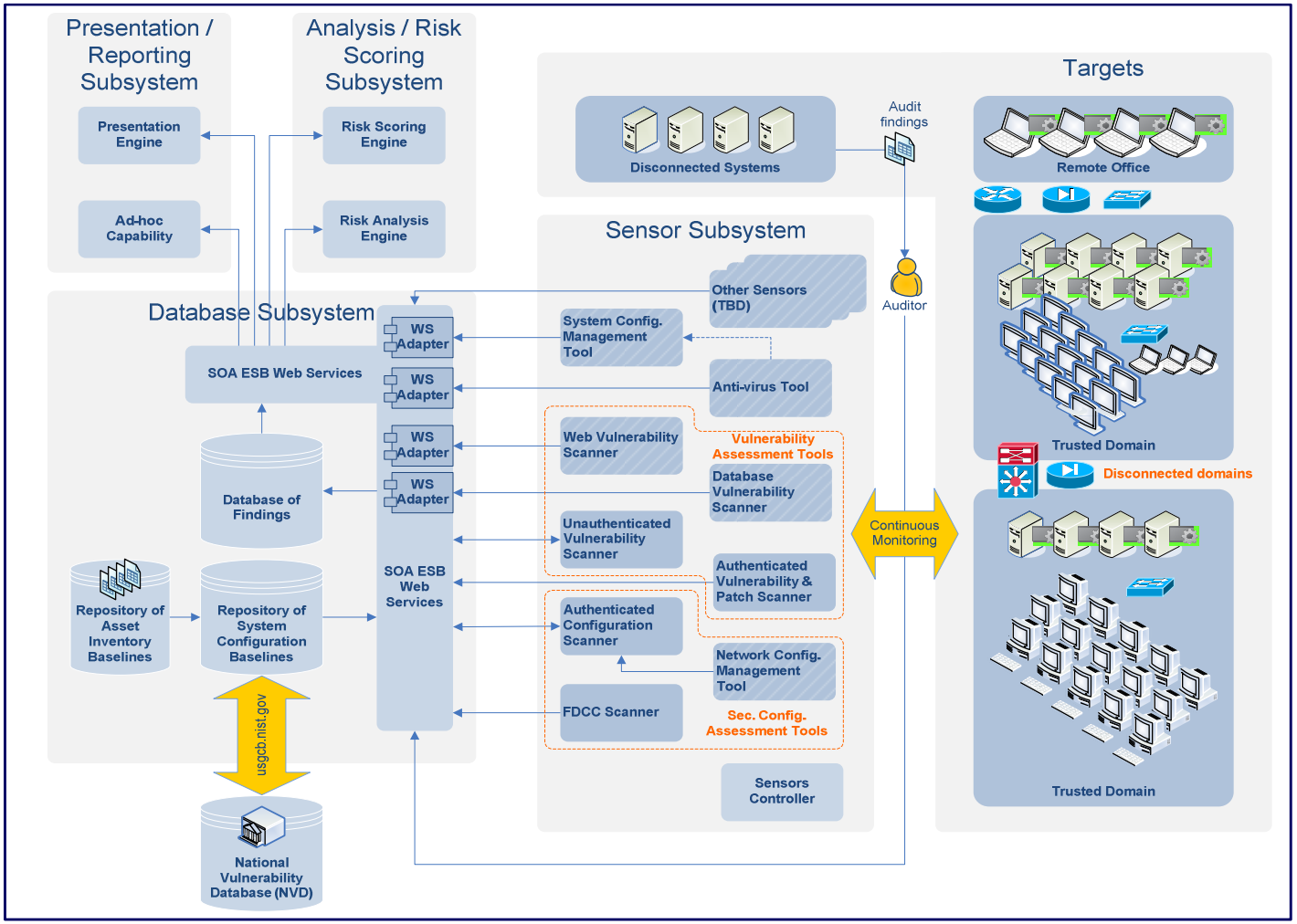
1. Leverage expertise and existing capabilities across government through the establishment of Shared Service Centers.

2. Partner with GSA to provide cost effective BPAs for IT security products and services via the SmartBUY Program.

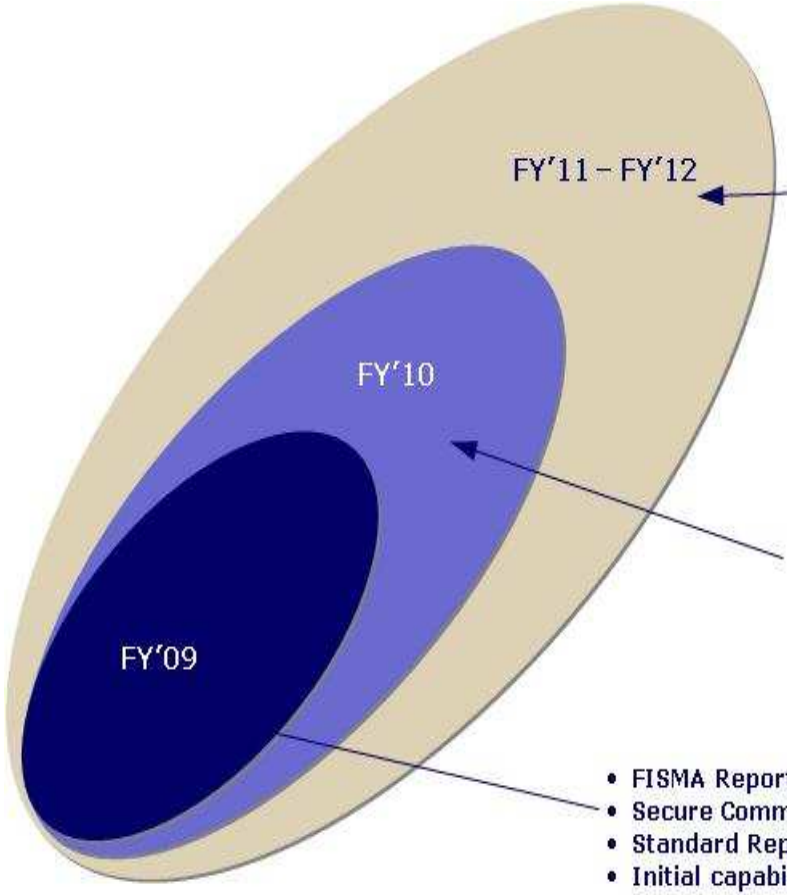
SAIR I	SAIR II	RMF
• Baseline Configuration • Network Mapping & Path Discovery • Vulnerability Management	• Web Application Firewall • End Point Protection • Data Flow Analysis • SIEM Tools	• End-to-End RMF Services in accordance with NIST RMF Guidance in SP 800-37 Revision 1

CAESARS* Reference Architecture:

***Continuous Asset Evaluation, Situational Awareness, and Risk Scoring**



CyberScope Evolution



- Incorporate emerging trends & security posture data
- Expand Automated Feeds to capture to routers, switches, non-windows OS, databases, non-windows software
- Potential to Expand classification of data (Nat'l Sec)
- Increase reporting intervals enhancing continuous monitoring

- Automate Capture of Desktop, Laptop & Server FDCC settings (SBU Only)
- Use Enhanced Performance Metrics
- Enhance Analytics
- Increased Reporting Capabilities (Quarterly, Monthly)
- Initial shift to Continuous Monitoring & Automated Feeds

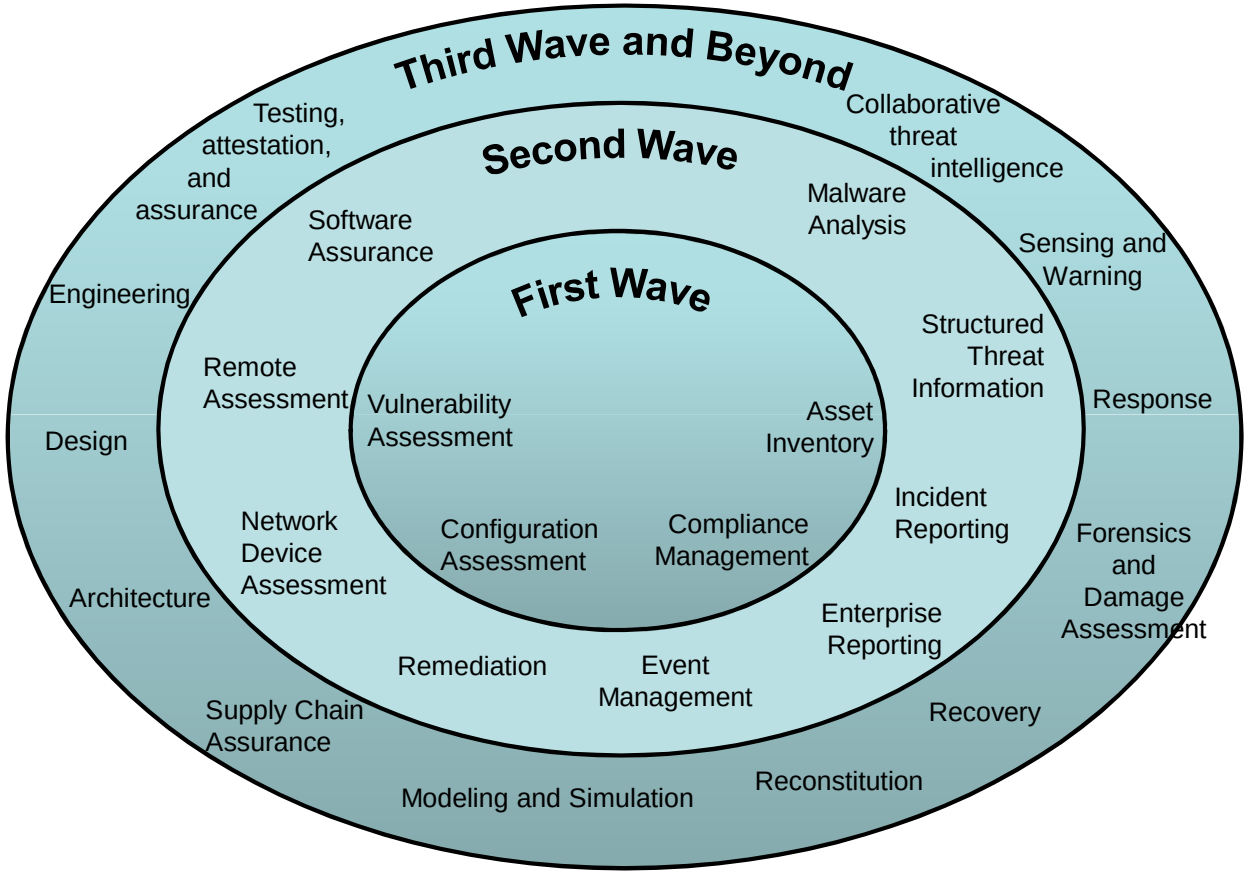
- FISMA Report Submission
- Secure Communication (PIV)
- Standard Reports
- Initial capability and repository

Homeland Security

FISMA Automation "Future Generations"

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

Ecosystem View



Ongoing Activities

- **Continuous Monitoring Working Group (CMWG) to collaboratively develop next iteration of FISMA metrics**
  - Prioritizing on data that is largely available today with existing tools
  - Will serve as baseline to drive additional standards, vendor adoption, content development, and procurement vehicles
- **Strategic Sourcing effort to expand continuous monitoring tools and services (SAIR TIER III)**
- **Update to CAESARS reference architecture for continuous monitoring**

- **Please join and contribute to the CMWG!**

Federal Network Security

Homeland Security