

Enclave Security: Secure Configuration Management (SCM)

<http://www.disa.mil/scm>

Agenda

- SCM Introduction
- SCM Lifecycle
- SCM Objectives
- SCM Community Model
- Current Capability Framework
- Governance Model
- Schedule
- Capability Program Map
- NSA SCM R&D Focused Efforts
- SCM Programs

Introduction

- Security-focused Configuration Management (SecCM) is defined as:

“the management and control of configurations for information systems to enable security and facilitate the management of information security risk.” (NIST SP 800-128)

PROGRAM OBJECTIVES:

- The DoD SCM Program is the integration and optimization of enterprise IA applications, tools, and data standards to support automated processes used to support risk management and near-real time awareness.
- Enables Information System Monitoring as part of DoD’s Continuous Monitoring Strategy – supporting the initial data sets of assets, system configurations, and vulnerabilities (FISMA reporting requirements).

PROGRAM CAPABILITIES:

- Leverage inherent SCM capabilities used within CC/S/As
- Provide pervasive enterprise capabilities and interfaced automated capabilities based on common data standards to enhance and accelerate CC/S/As ability to:
 - Identify assets
 - Check system configuration compliance against policies and standards
 - Search for potential vulnerabilities
 - Act on known vulnerabilities for known risk posture for system/networks
 - Report status & share information with those that need to know

*Configure assets securely; Maintain secure Configurations;
Provide continuous situational awareness to the right people*

Why SCM?

The Enterprise Today:

- Difficult to maintain secure configurations: high level of effort, diminished return on investment
- Disparate IA tool sets: proprietary capabilities, disconnected and stand-alone configurations
- Manual reporting: resource intensive, slow, and limits trusted situational awareness



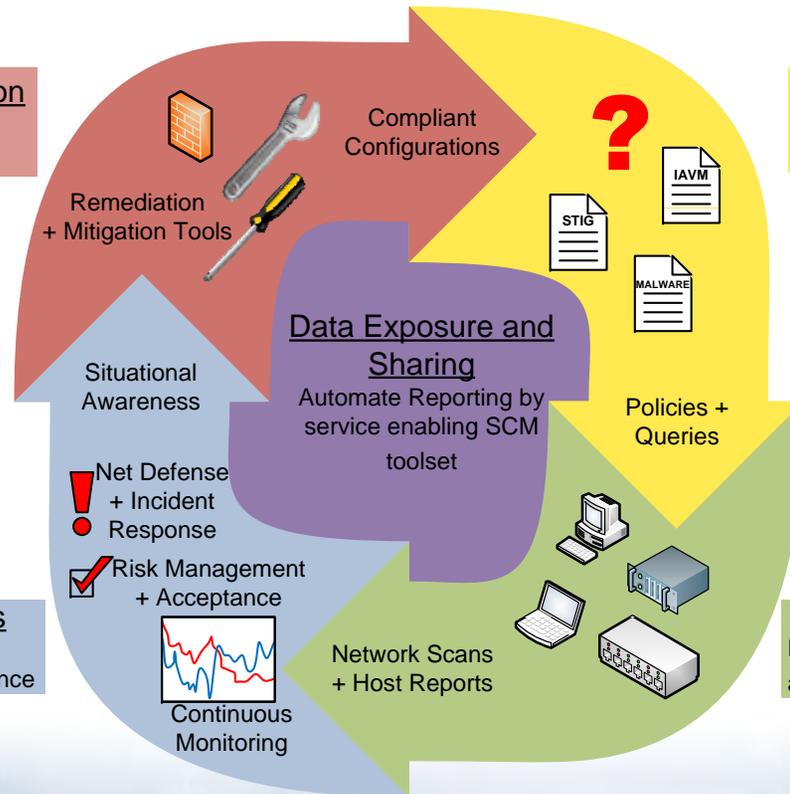
The Future Enterprise:

- Automated, end-to-end security compliance process
- Standardized and validated toolsets connected throughout the enterprise
- Continuous reporting to improve data integrity and validity



SCM Lifecycle

Configuration Risk Mitigation
Allow for the remediation of non-secure configurations



Security Content Management
Create and distribute content for vulnerability and configuration tools

Security State Analysis
Assess risk by correlating asset attributes and compliance evidence

Configuration Discovery and Detection
Discover and audit assets with standardized, automated tools

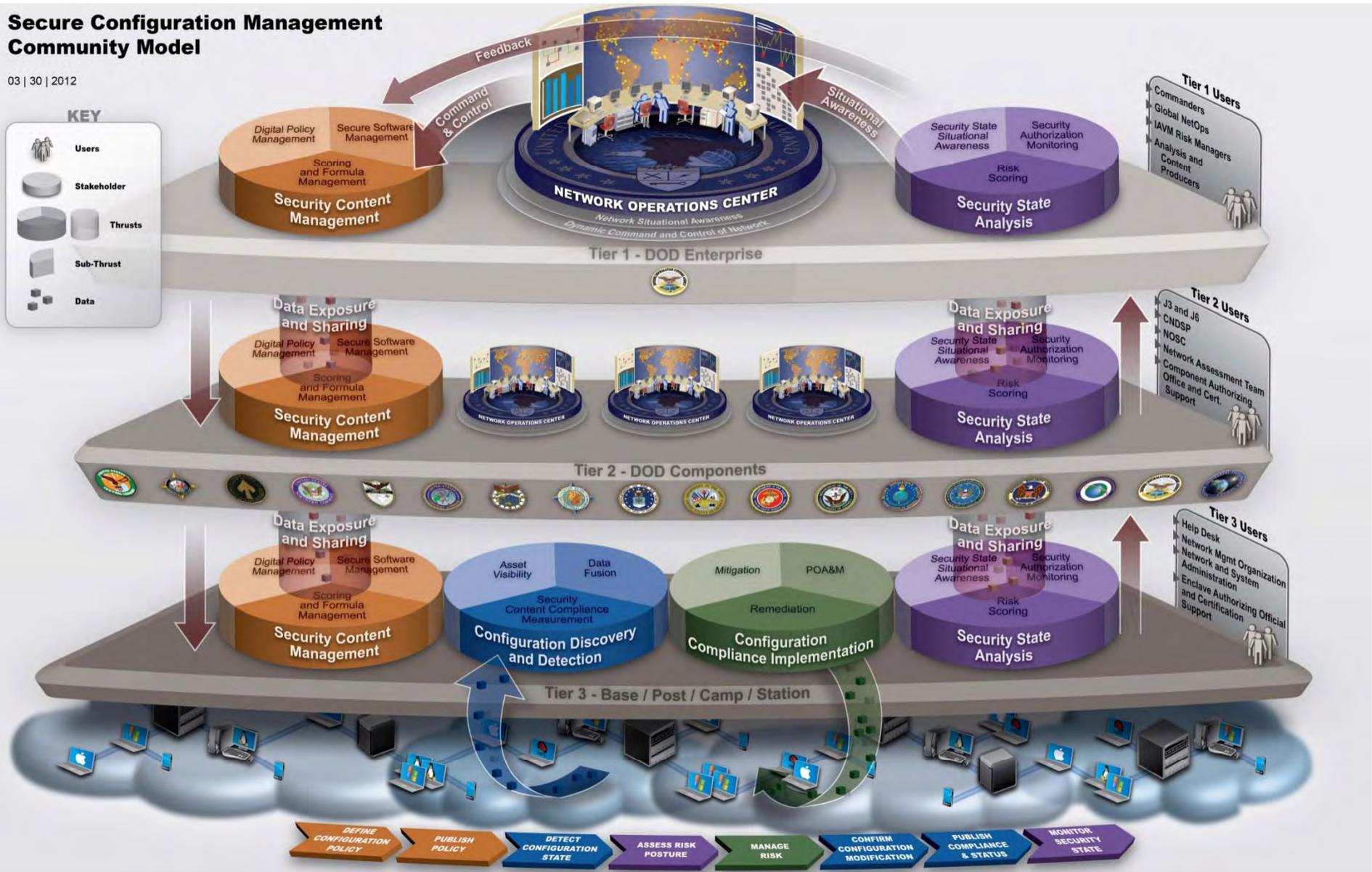
SCM Program Objectives

- **The SCM Program implements published standards, using validated tools and employs standardized interfaces to realize essential Secure Configuration capabilities.**
- Standards: Secure Configuration Automation Protocol (SCAP). A NIST-developed, industry-adopted set of standards supporting interoperability and automated data exchange. Extended to include standard data formats for reporting asset and summary information.
- Tools: Commercial-off-the-Shelf (COTS) and Government-off-the-Shelf (GOTS) tools validated as conforming to SCAP standards.
- Interfaces: Leverage SCAP and emerging standards (Asset Report Format (ARF) / ARF Summary Report (ASR)) to distribute asset data by defining data input and output formats for SCAP-validated tools
- Capabilities: Content/Policy development; Asset Inventory/Discovery; Security State Analysis/Risk Assessment; and Risk Mitigation

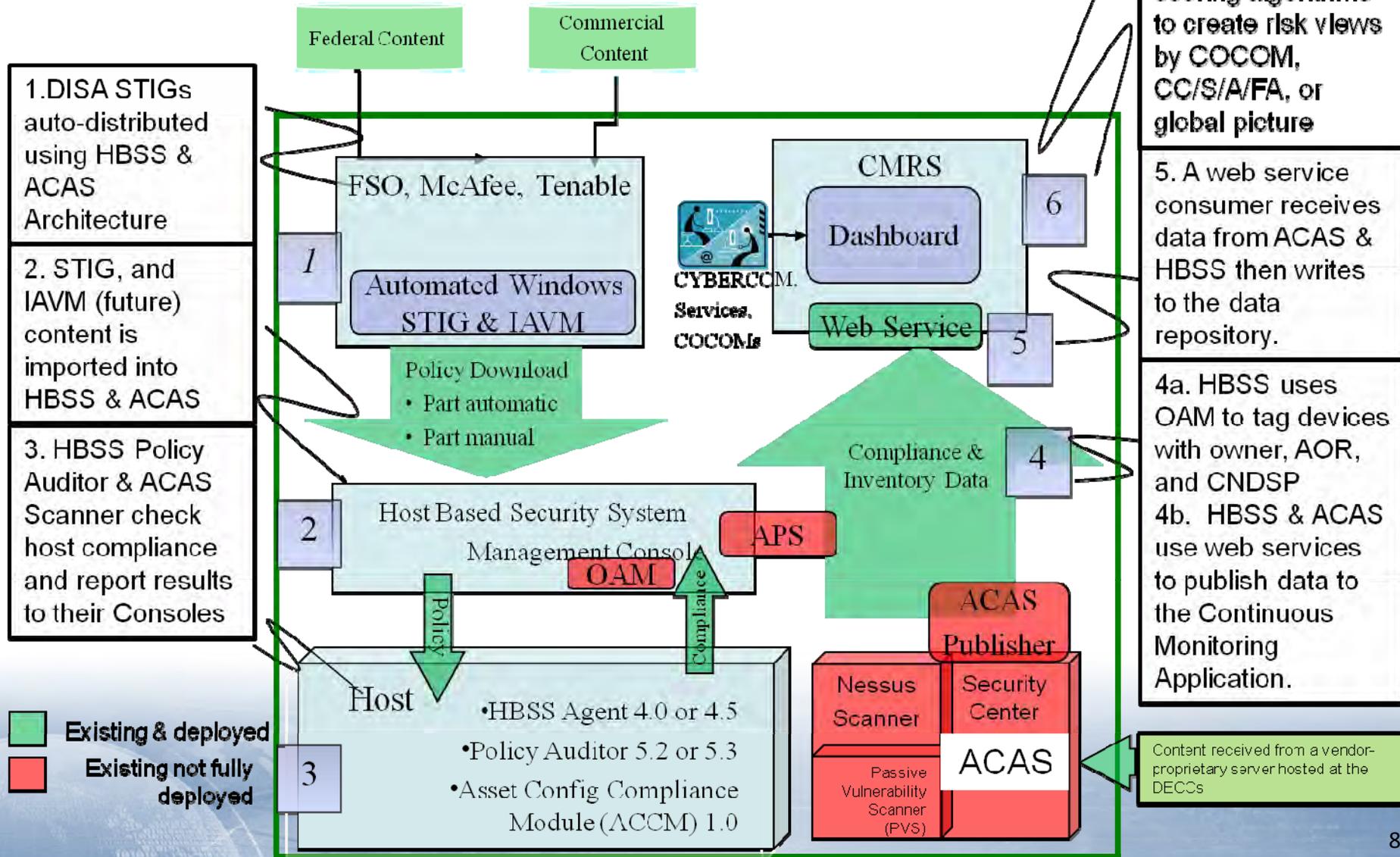
SCM Community Model

Secure Configuration Management Community Model

03 | 30 | 2012



Near-Term SCM Capability Framework

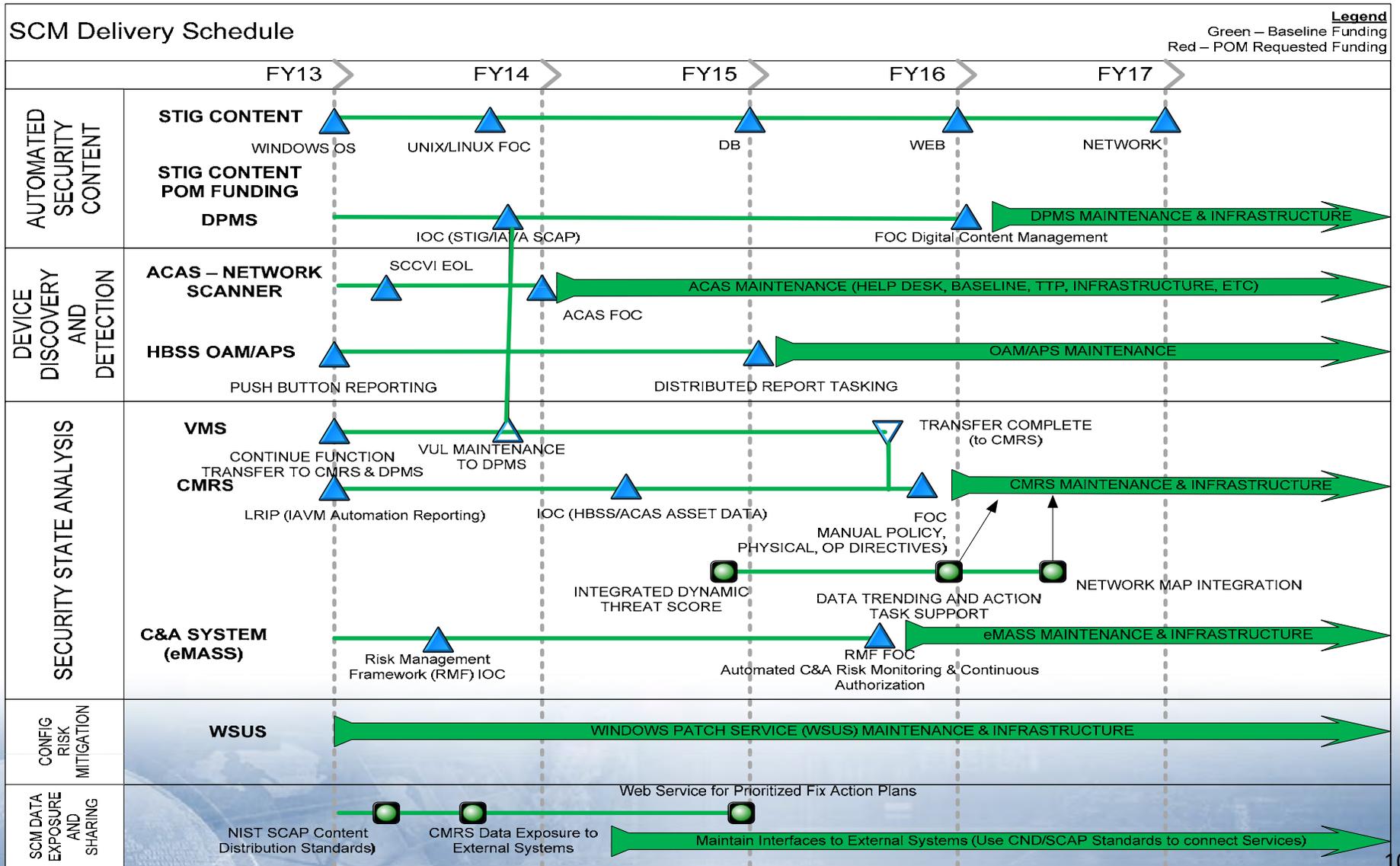


SCM Governance Model

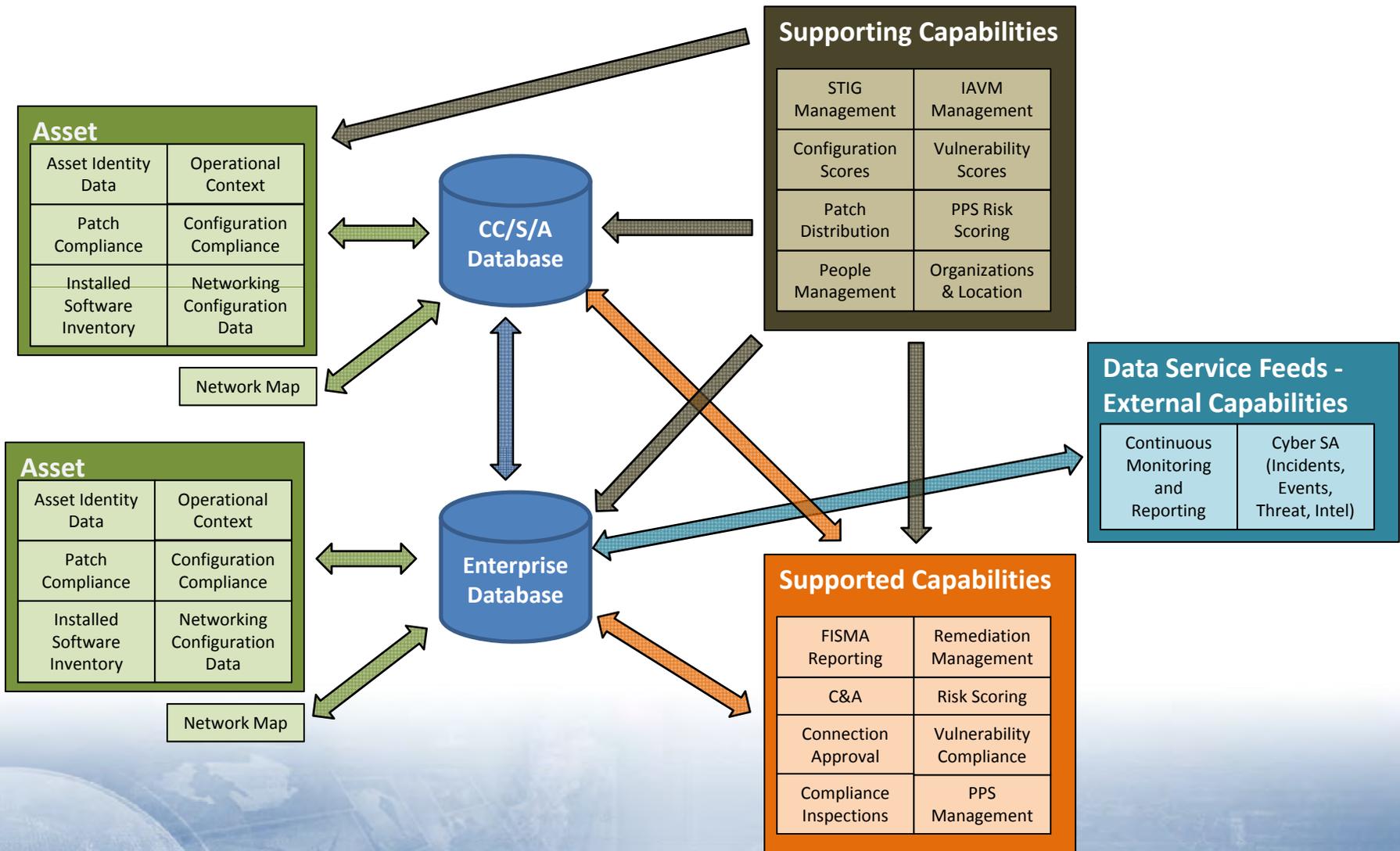




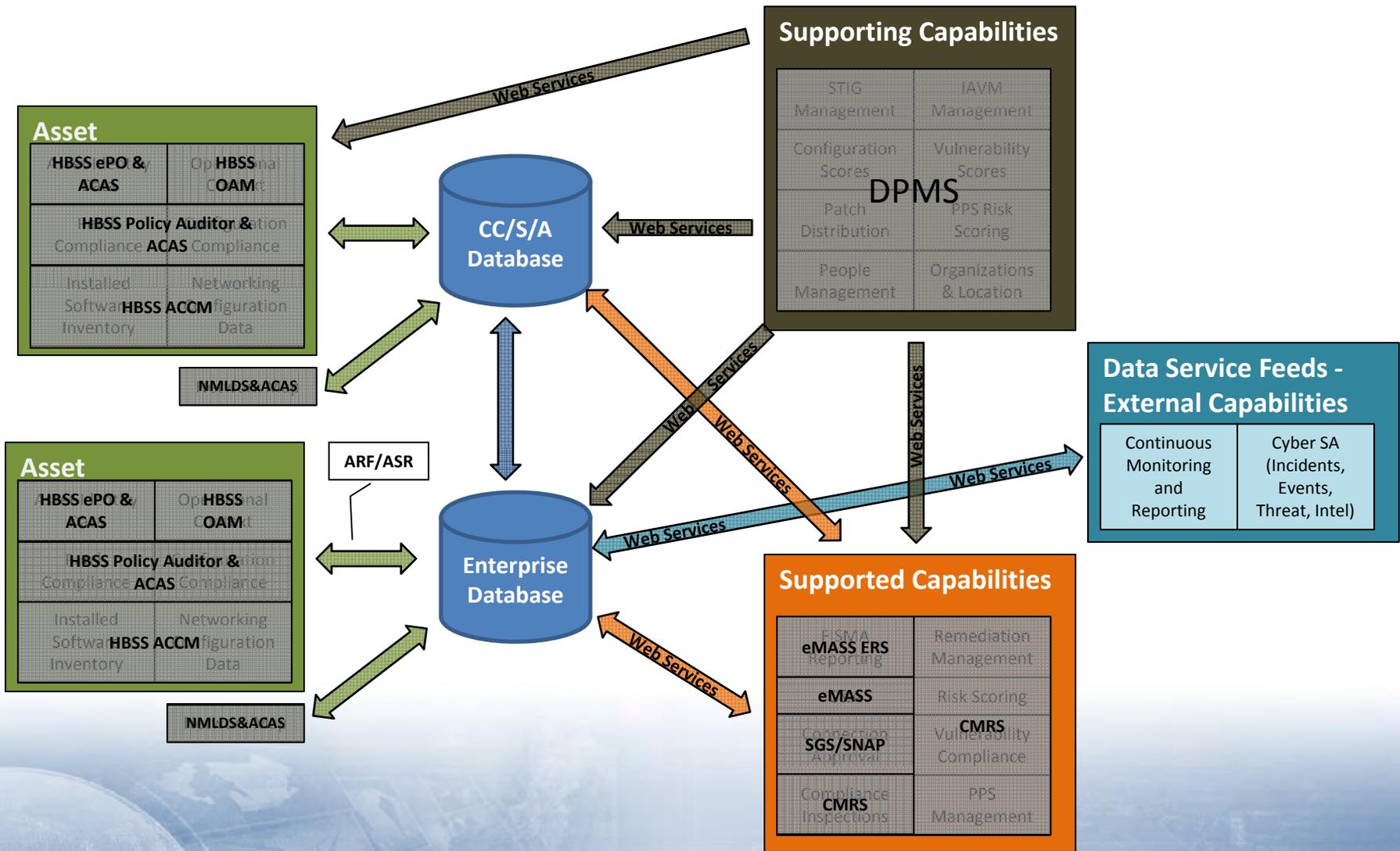
SCM Capability Initiatives and Evolution



SCM Capability Map



SCM Program Overlay





(U) SCM Research and Development NSA Focus Areas (from POM13 process)

- **(U) SCM in a Virtualized Environment:** Development and testing of Secure Configuration Management tools and concepts in both persistent and non-persistent virtual environments
- **(U) SCM in a Mobile Environment:** Development and testing of Secure Configuration Management tools and concepts in wireless and mobile environments (mobile devices)
- **(U) Automated Remediation:** Development of remediation policies, standards and techniques that allow for both centralized and decentralized control of remediation and mitigation capabilities
- **(U) Human Sensor (OCIL):** Develop automated capabilities and standards (Open Checklist Interactive Language) to collect IT asset and configuration relevant data from human sensors
- **(U) Additional SCAP Development :**Development, piloting, and testing of reference content in support of other R&D SCM efforts

(U) Focus Areas for SCM Research and Development chosen to help drive Enterprise SCM Architecture at DISA

DISA SCM Programs





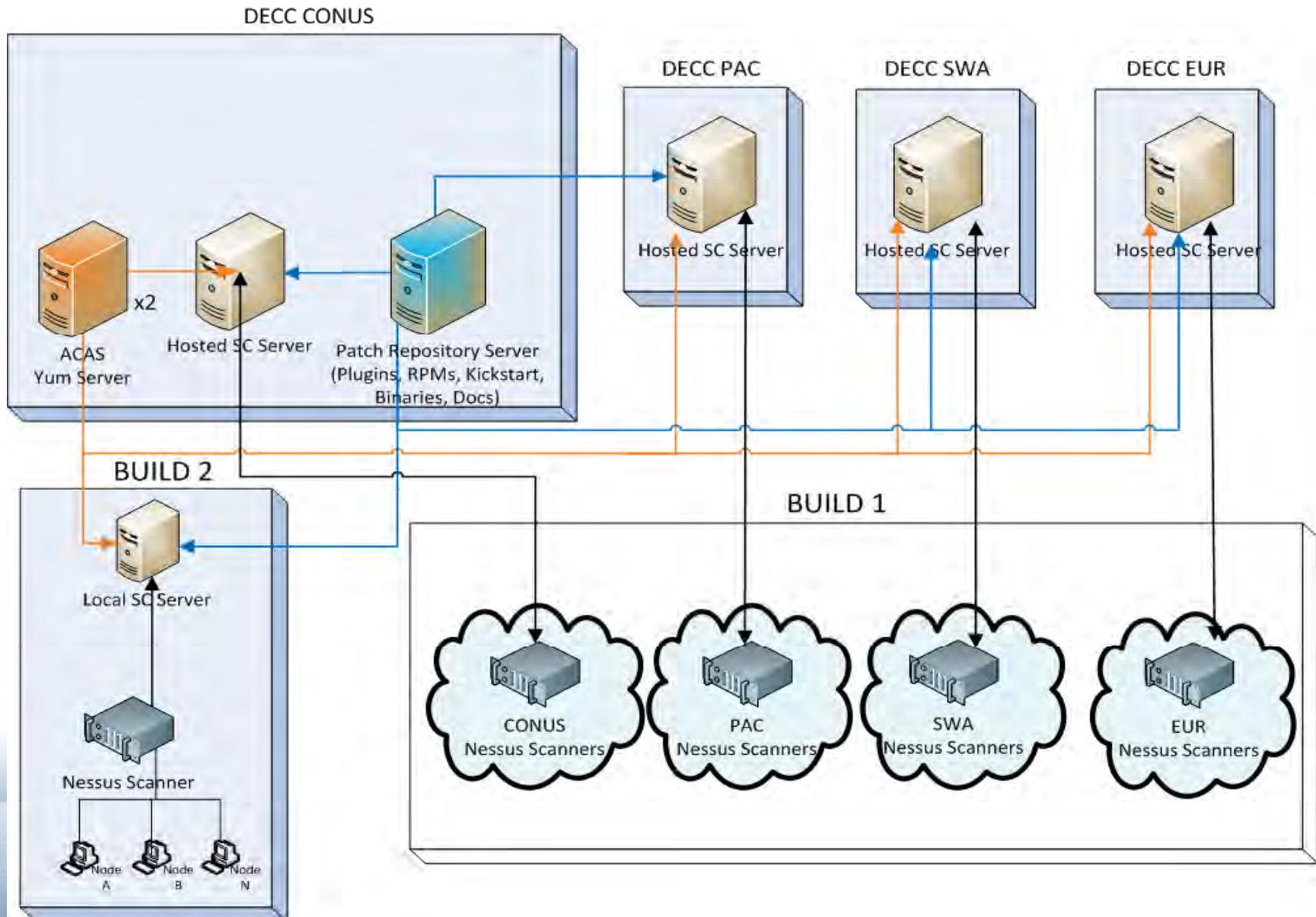
SCM Enterprise Tools and Services

- ACAS
- CMRS/PRSM
- DPMS
 - IAVM Service
 - VMS STIG Maintenance
 - Patch Repository
 - Severity Scoring
- eMASS
- ENMLDS
- HBSS
 - Policy Auditor
 - OAM
 - APS
 - ACCM
- Remediation Manager
- VMS

ACAS

- Assured Compliance Assessment Solution (ACAS)
 - An integrated *software* solution that provides automated network vulnerability scanning, configuration assessment, application vulnerability scanning, device configuration assessment, and network discovery
 - Five components make up the ACAS solution
 - SECURITYCENTER - the central console that provides continuous asset-based security and compliance monitoring
 - NESSUS VULNERABILITY SCANNER - features discovery, configuration auditing, and vulnerability analysis
 - PASSIVE VULNERABILITY SCANNER - performs real-time network traffic monitoring
 - X-TOOL - converts XCCDF/OVAL files into XML schema
 - TOPOLOGY VIEWER (3D Tool) - provides a graphical network map
 - Contract awarded to HP Enterprise Services partnering with Tenable

ACAS Architecture





ACAS Portals

- ACAS WIKI
 - <https://www.intelink.gov/wiki/ACAS>
- ACAS Front Door-
 - <http://www.disa.mil/Services/Information-Assurance/SCM/ACAS>
- DOD Patch Management Server
 - <https://patches.csd.disa.mil>



Continuous Monitoring and Risk Scoring (CMRS)

Priority Description

- CMRS is the development and implementation of an Enterprise DoD system for Blue Force Tracking of the DoD IT infrastructure to enable risk-based deployment & C2 of DoD protective & defensive resources

Objective

Integrate and optimize DoD Enterprise IA applications, tools, and data standards to provide near-real time risk management, automated configuration management, and continuous monitoring capabilities that optimize net defense and risk awareness for information systems (computing assets, applications, and networking devices) .

- Configure assets securely
- Maintain secure configurations
- Provide continuous situational awareness to the right users

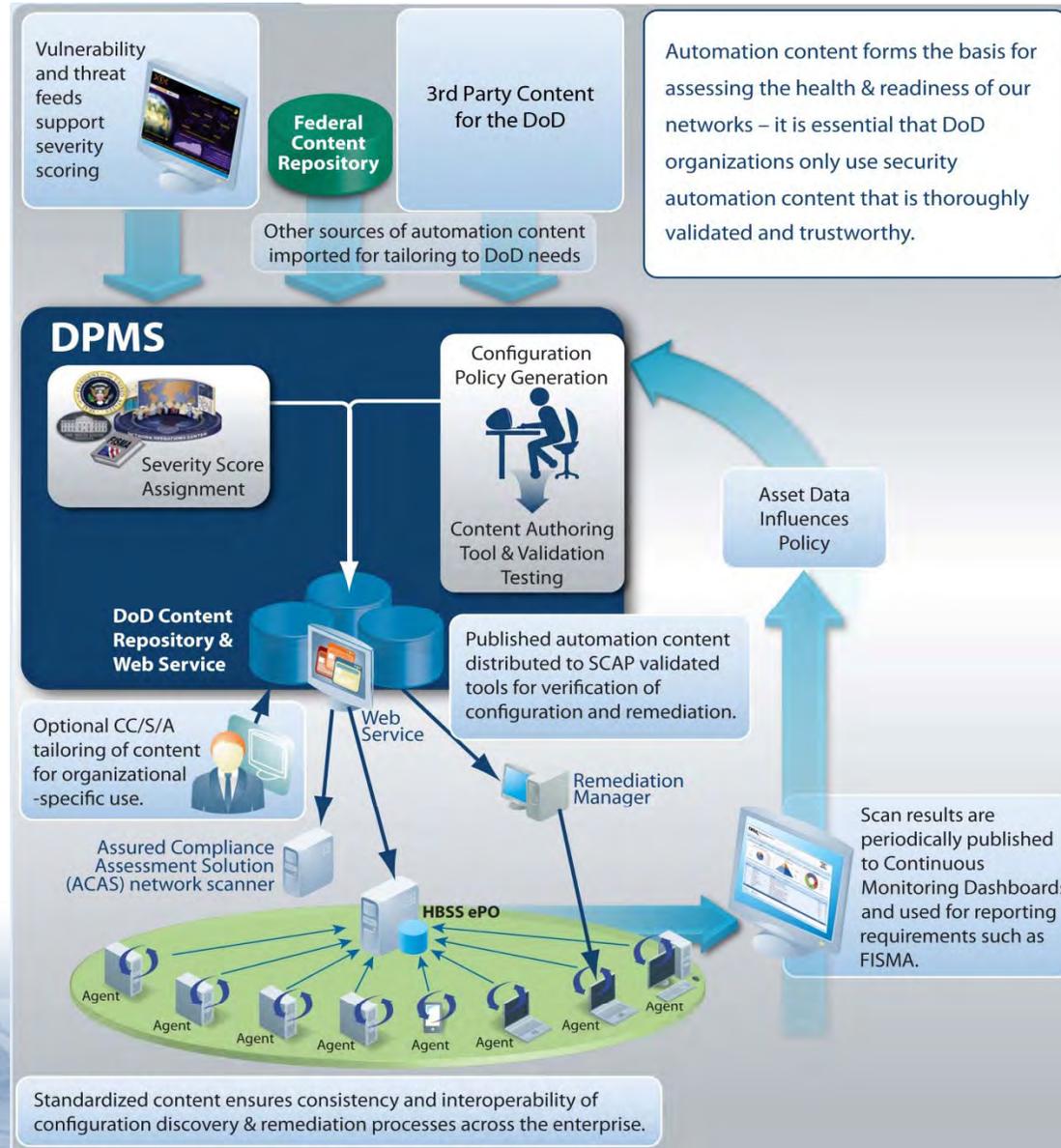
Operational Status

- Pre-IOC infrastructure for automated and continuous IAVM Reporting (CMRS)
- Collection and Analysis of CMRS Requirements
- CMRS Pilot Development & Maintenance
- Deployed on DISA NIPRNet/SIPRNet

Way Ahead

- **Q4FY12**- CMRS operationalized to support Windows IAVM automation
- **Q1FY13** – COCOM view of security compliance status (STIG, IAVM, AV/AS)
- **Q1FY13** – CMRS support for Solaris and Red Hat IAVM Automation
- **Q2FY13**- Begin data service feeds for C&A automation
- **Q4FY13**- CMRS to support non automated compliance checks
- **Q4FY13** – Automated ACAS reporting for IAVM and compliance of network devices
- **Q4FY13** – CMRS Enterprise infrastructure IOC (Scale to an enterprise solution to allow for standards based network scanning, automated SCAP policy distribution to HBSS)
- **Q4FY14**- Implement Dynamic Risk Scoring based on current threats
- **Q1FY15**- CMRS integrated with remediation management system
- **Q4FY15**- CMRS FOC

Digital Policy Management System (DPMS)



eMASS

- eMASS is a GOTS tool providing easy to use C&A workflow tool and simplified development of DIACAP packages
- Consumes asset data from SCM enabling continual re-assessment of accredited systems versus periodic inspections
- Provides dashboard visibility of enterprise IA posture as well as system-specific compliance status
- Can be leveraged for FISMA reporting and reporting to DITPR

ENMLDS

- Enterprise Network Mapping and Leak Discovery Solution
 - The Enterprise Network Mapping and Leak Detection Solution (ENMLDS) provides administrators and security personnel with the capability to identify and graphically represent the components that exist on a network. The capability will assist DoD organizations in discovery of unauthorized entry or exit points in their network.
 - Provides a picture of what's actually connected in the environment, not just what's believed to be there
 - A scalable mapping solution for large, disparate networks
 - Provides visibility into rogue connectivity
 - Highlights network misconfiguration which expose the GIG



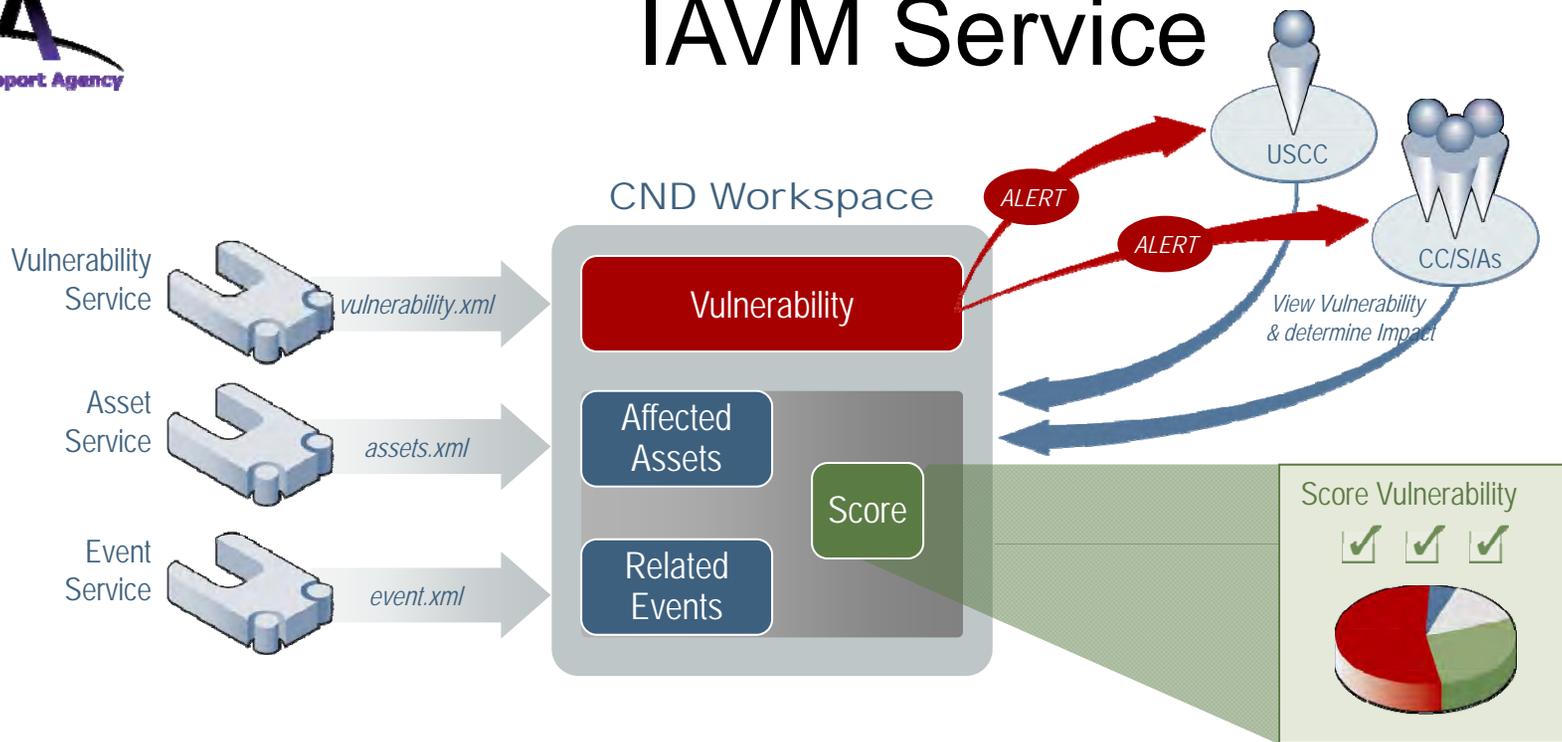
Asset Configuration Compliance Module (ACCM)

- ACCM 1.0 *inventories* all installed applications, operating systems, and patches/updates that are on Windows machines (MR3)
 - ACCM 1.0, initial release does not report via APS up-tier
- ACCM 2.0 will *compute compliance* with external and internal policies (MR4)
 - Also support for RHEL, Mac OSX, and Solaris

HBSS SCM Products

- Operational Attributes Module
 - Capability to assign attributes to system tree groups in HBSS
 - Support or organizations, AOR, CNDSP, System/POR, Network, etc...
- Policy Auditor
 - McAfee, SCAP-validated authenticated host scanning tool
- Asset Configuration Compliance Module (ACCM)
 - Version 1.x Inventories installed applications, operating systems, and patches/updates on MS Windows hosts and collects detailed network interface configuration data.
 - Version 2.0 adds support for RHEL, Mac OSX, and Solaris
- Asset Publishing Service
 - Publishes asset identity, operational attributes, sw inventory, and Policy Auditor results to a consuming web service using ARF and ASR data formats

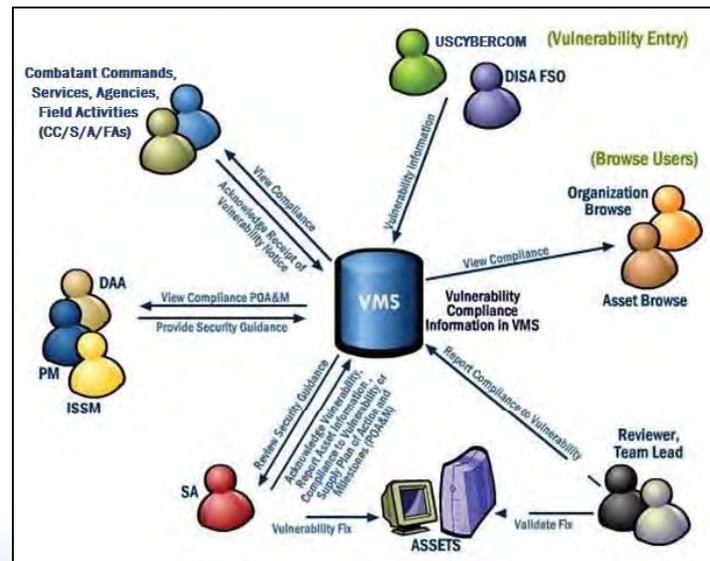
IAVM Service



- The IAVM Service is a web-based application to accelerate and automate the DoD's vulnerability assessment and IAVM notice creation processes.
 - Features a standards-based user interface to automate data correlation between vulnerabilities and DoD assets
 - Allows for analysts to score vulnerabilities utilizing Common Vulnerability Scoring System (CVSS)
 - Allows analysts to watch, track and reprioritize vulnerabilities
 - Allows analysts to create, issue, expire and retire IAVMs

Vulnerability Management System

- VMS is an enterprise web application hosted in a CSD DECC
 - Organizational and program level tracking of STIG and IAVM asset compliance and POA&Ms
 - Tracks compliance of USSTRATCOM Operational Directives and IAVMs for each CC/S/A
 - Tracks CCRI results* (used in conjunction with NetOps Directive Tracking System (NDTS))
- SCM Integration
 - VMS modified to ingest data from HBSS Policy Auditor and OAM to update asset STIG/IAVM compliance.
 - VMS combines machine reported compliance data with manually reported asset compliance. E.g., physical security, non-automatable technical checks.
- VMS Functions will be maintained as SCM Program evolves to enterprise continuous monitoring and risk scoring capabilities



SCM Components

- Antivirus/Antispyware – Antivirus and Antispyware products for DoD
- Asset Configuration Compliance Module (ACCM) – HBSS module to perform system software inventory using SCAP Common Platform Enumerations (CPE)
- Asset Data Service (ADS) – Web application to collect bulk asset records and attributes from HBSS and other CC/S/A asset management systems.
- Asset Publishing Service (APS) – HBSS module to publish SCAP compliance data to the NCES JUM.
- Assured Compliance Assessment Solution (ACAS) – SCAP validated network vulnerability assessment tool.
- Automatable STIG Publication – VMS capability to publish SCAP STIGs (XCCDF/OVAL)
- Continuous Monitoring and Risk Scoring (CMRS) – Web services and applications to collect machine to machine SCAP data to present common risk scores and AOR/UNIT compliance scores. (e.g., Dept. of State iPOST)
- Digital Policy Management Service (DPMS) – Consolidated system to manage the creation, maintenance, and distribution of STIGs, IAVMs, SCAP content, Patches, HIPs signatures. Combining and merging partial capabilities of VMS, IAVM System, eSCAPE, Patch Service.
- Enterprise Network Mapping and Leak Detection Solution (ENMLDS) – Enterprise network mapping, host discovery, and domain leak detection.
- Enterprise Mission Assurance Support Service (eMASS) –DIACAP support web application
- Gold Disk – DoD GOTs product to perform Windows STIG/IAVM assessments and remediation

SCM Components (cont)

- Host Based Security System (HBSS) – RSD, PA, ePO Rollup, OAM
 - RSD – reports rogue, unmanaged hosts on ePO managed networks.
 - Policy Auditor – SCAP validated agent-based tool that assesses host security compliance
 - ePO Rollup – HBSS reporting capability that reports to the Tier 1
 - OAM – HBSS module to allow assignment of operational attributes to host records.
- IAVM System – Collaborative IAVM pre-coordination web site for CC/S/A to input information related to pending IAVM issuances.
- Patch Management, WSUS – Enterprise patch distribution web server and Windows patch service
- Ports, Protocols, and Services (PPSM DB) – Web application to track risk associated to well-known network ports, protocols, and services (PPS). Supports the registration and tracking of approved application PPS.
- Remediation / Remediation Manager – Potential follow on to SCRI. Pending the definition of enterprise requirements, the Remediation program may be a remediation policy manager to manage approved or recommended mitigations/remediation or a remediation tool to perform remediation/mitigations on hosts.
- Secure Configuration Compliance Validation Initiative (SCCVI) – Network vulnerability assessment tool.
- Secure Configuration Remediation Initiative (SCRI) – Enterprise patch and remediation tool.
- Vulnerability Management System (VMS) – Web application to track Operational Directive acknowledgement and compliance, IAVM compliance, and STIG compliance for technical and non-technical assets.

QUESTION

