

# Leveraging Automation to Enhance FISMA: *Use of Security Automation Standards*

Jon Baker

[bakerj@mitre.org](mailto:bakerj@mitre.org)

September 13, 2011

# Overview

- **FY11 CIO FISMA Reporting Metrics Use of Security Automation Standards**
  - What standards are referenced?
  
- **Describe the referenced security automation standards**
  - What are they?
  
- **Motivators: SANS Top 20 Critical Security Controls and Continuous Monitoring**
  - Why do we need security automation standards?

# FY11 CIO FISMA Reporting Metrics: *Use Of Security Automation Standards*

- **Section 2: Asset Management**
  - SCAP for Asset Inventory (CPE & OVAL)
- **Section 3: Configuration Management**
  - SCAP for describing the desired configuration (XCCDF, CPE, CCE, & OVAL)
- **Section 4: Vulnerability Management**
  - CVE for identifying software vulnerabilities
  - SCAP for describing vulnerable configuration (CVE, CVSS, & OVAL)
- **Section 12: Software Assurance**
  - CWE for identifying software flaws
  - CVE for identifying software vulnerabilities
  - CVSS for identifying the most important software vulnerabilities
  - OVAL for checking for known vulnerabilities and misconfigurations
- **Section 13: Continuous Monitoring**
  - Standard languages and identifiers enable automated assessments, responses, and other advanced analytics.

## Section 2. ASSET MANAGEMENT

- **2.1. Provide the total number of Agency Information Technology assets (e.g. router, server, workstation, laptop, blackberry, etc.).**
  - 2.1a. Provide the number of Agency information technology assets, connected to the network, (e.g. router, server, workstation, laptop, , etc.) where an automated capability provides visibility at the Agency level into asset inventory information.
  - 2.1b. Provide the number of Agency information technology assets where an automated capability produces **Security Content Automation Protocol (SCAP) compliant asset inventory information output.**
  - 2.1c. Provide the number of Agency information technology assets where all of the following asset inventory information is collected: Network address, Machine Name, Operating System, and Operating System/Patch Level.
- **2.2. Has the Agency implemented an automated capability to detect and block unauthorized software from executing on the network?**
- **2.3. Has the Agency implemented an automated capability to detect and block unauthorized hardware from connecting to the network?**
- **2.4. For your Agency, which type(s) of assets are the most challenging in performing automated asset management? Rank the asset types below from 1---4 with 1 being the most challenging.**
  - 2.4a. Servers
  - 2.4b. Workstations/Laptops
  - 2.4c. Network Devices
  - 2.4d. Mobile Devices

# Section 3. CONFIGURATION MANAGEMENT

- **3.1. Provide the number of Agency information technology assets where an automated capability provides visibility at the Agency level into system configuration information (e.g. comparison of Agency baselines to installed configurations).**
  - 3.1a. Provide the number of Agency information technology assets where an automated capability produces **SCAP compliant system configuration information output.**
- **3.2. Provide the number of types of operating system software in use across the Agency**
  - 3.2a. Provide the number of operating system software in use across the Agency for which standard security configuration baselines are defined. Consider an Agency approved deviation as part of the Agency standard security configuration baseline.
- **3.3. Provide the number of enterprise---wide applications (e.g., Internet Explorer, Adobe, MS Office, Oracle, SQL, etc.) in use at the Agency.**
  - 3.3a. Provide the number of enterprise---wide applications for which standard security configuration baselines are defined. Consider an Agency approved deviation as part of the Agency standard security configuration baseline.

## Section 4. VULNERABILITY MANAGEMENT

- **4.1. Provide the number of Agency information technology assets where an automated capability provides visibility at the Agency level into detailed vulnerability information (Common Vulnerabilities and Exposures -- CVE).**
  - 4.1a. Provide the number of Agency information technology assets where an automated capability produces **SCAP compliant vulnerability information output.**

## Section 12. SOFTWARE ASSURANCE

- **12.1 Provide the number of information systems, developed in--house or with commercial services, deployed in the past 12 months.**
  - 12.1a. Provide the number of information systems above (12.1) that were **tested using automated source code testing tools**. (Source code testing tools are defined as tools that review source code line by line to detect security vulnerabilities and provide guidance on how to correct problems identified.)
  - 12.1b. Provide the number of the information systems above (12.1a) where the tools generated output compliant with:
    - **12.1b(1). Common Vulnerabilities and Exposures (CVE)**
    - **12.1b(2). Common Weakness Enumeration (CWE)**
    - **12.1b(3). Common Vulnerability Scoring System (CVSS)**
    - **12.1b(4). Open Vulnerability and Assessment Language (OVAL)**

# Section 13. CONTINUOUS MONITORING

- **13.1. What percentage of data from the following potential data feeds are being monitored at appropriate frequencies and levels in the Agency:**
  - 13.1a. IDS/IPS
  - 13.1b. AV/Anti---Malware/Anti---Spyware
  - 13.1c. System Logs
  - 13.1d. Application logs
  - 13.1e. Patch Status
  - 13.1f. Vulnerability Scans
  - 13.1g. DNS logging
  - 13.1h. Configuration/Change Management system alerts
  - 13.1i. Failed Logins for privileged accounts
  - 13.1j. Physical security logs for access to restricted areas
  - 13.1k. Data Loss Prevention data
  - 13.1l. Remote Access logs
  - 13.1m. Network device logs
  - 13.1n. Account monitoring
    - 13.1n(1). Locked out
    - 13.1n(2). Disabled
    - 13.1n(3). Terminated personnel
    - 13.1n(4). Transferred personnel
    - 13.1n(5). Dormant accounts
    - 13.1n(6). Passwords that have reached the maximum password age
    - 13.1n(7). Passwords that never expire
  - 13.1o. Outbound traffic to include large transfers of data, either unencrypted or encrypted.
  - 13.1p. Port scans
  - 13.1q. Network access control lists and firewall rule sets.
- **13.2 To what extent is the data collected, correlated, and being used to drive action to reduce risks? Please provide a number on a scale of 1---5, with 1 being that “All continuous monitoring data is correlated”.**

# More on the standards...

**SCAP**

	<b>CVE</b>	Common Vulnerabilities & Exposures	Standard nomenclature and dictionary of security vulnerabilities	<b>Naming</b>
	<b>CCE</b>	Common Configuration Enumeration		
	<b>CPE</b>	Common Platform Enumeration	Standard nomenclature and dictionary for product naming	
	<b>XCCDF</b>	eXtensible Checklist Configuration Description Format	Standard format for expressing security configurations	<b>Expressing</b>
	<b>OVAL</b>	Open Vulnerability and Assessment Language	Standard format for expressing security assessments	<b>Assessing</b>
<b>OCIL</b>	<b>OCIL</b>	Open Checklist Interactive Language	Standard format for expressing security assessments to an end user	
	<b>CVSS</b>	Common Vulnerability Scoring System	Standard format for expressing vulnerability scores	<b>Scoring</b>
	<b>CWE</b>	Common Weakness Enumeration	Standard nomenclature and dictionary of security weaknesses	<b>Naming</b>

# Security Content Automation Protocol (SCAP)

A suite of seven preexisting open specifications that standardize the format and nomenclature by which security software communicates information about software flaws and security configurations.

- **Defines how these specifications are used in concert for the following activities:**

- vulnerability and patch management
- policy compliance evaluation
- asset inventorying
- detecting system compromise

- **Motivating factors:**

- Number and variety of systems to secure
- Need to respond quickly to new threats
- Lack of interoperability
- Complexity of guidance
- Number of security-related configuration settings
- Need to verify the security posture regularly

***“SCAP was created to provide a standardized approach to maintaining the security of enterprise systems, such as automatically verifying the presence of patches, checking system security configuration settings, and examining systems for signs of compromise.”***

NIST SP 800-117

# Layering the Security Automation Standards

**Policy**



**What?**



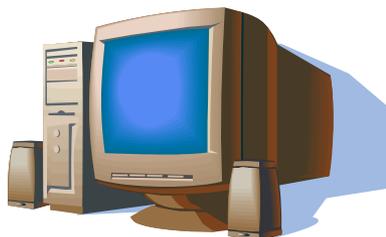
**Why?**



**Assess**



*OCIL*



# WHY?



**“...transform security in government agencies and other large enterprises by focusing their spending on the key controls that block known attacks and find the ones that get through.”**

- **Enabling agreement between those responsible for compliance and those responsible for security.**
- **The Top 20 Controls were developed by a consortium including:**
  - NSA, US Cert, DoD, the Department of Energy Nuclear Laboratories, Department of State, industry experts
- **Automation of these Top 20 Controls will radically lower the cost of security while improving its effectiveness.**
  - Department of State iPost demonstrated more than 80% reduction in "measured" security risk



## Critical Controls Subject to Automated Collection, Measurement, and Validation:

1. Inventory of Authorized and Unauthorized Devices
2. Inventory of Authorized and Unauthorized Software
3. Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers
4. Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
5. Boundary Defense
6. Maintenance, Monitoring, and Analysis of Security Audit Logs
7. Application Software Security
8. Controlled Use of Administrative Privileges
9. Controlled Access Based on Need to Know
10. Continuous Vulnerability Assessment and Remediation
11. Account Monitoring and Control
12. Malware Defenses
13. Limitation and Control of Network Ports, Protocols, and Services
14. Wireless Device Control
15. Data Loss Prevention

**SCAP Enables  
Automation**

Information security continuous monitoring is defined as maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. (NIST 800-137)

- **A result of numerous events coming together:**

- iPost: Implementing Continuous Risk Monitoring at the DoS
- SANS Top 20 Critical Controls (CAG)
- OMB FISMA Reporting Memo (M-10-15)

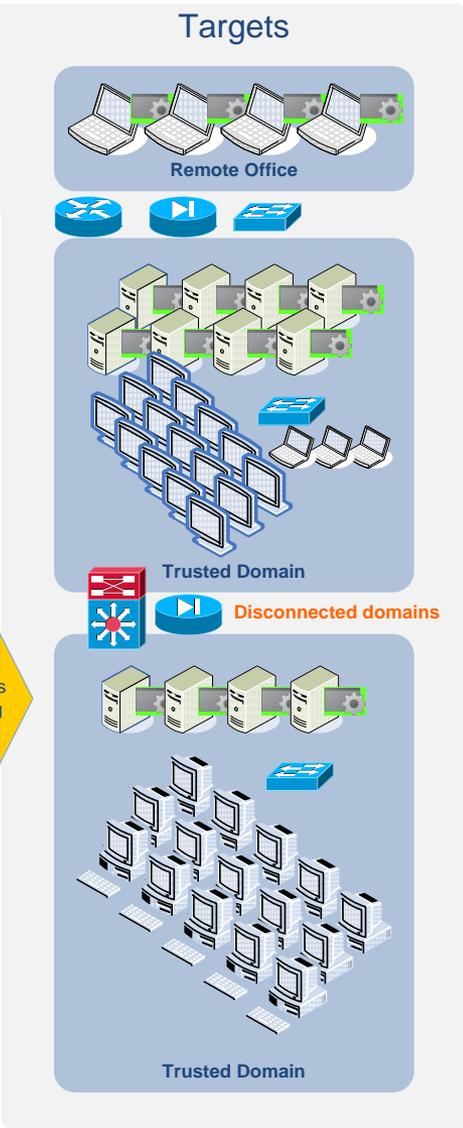
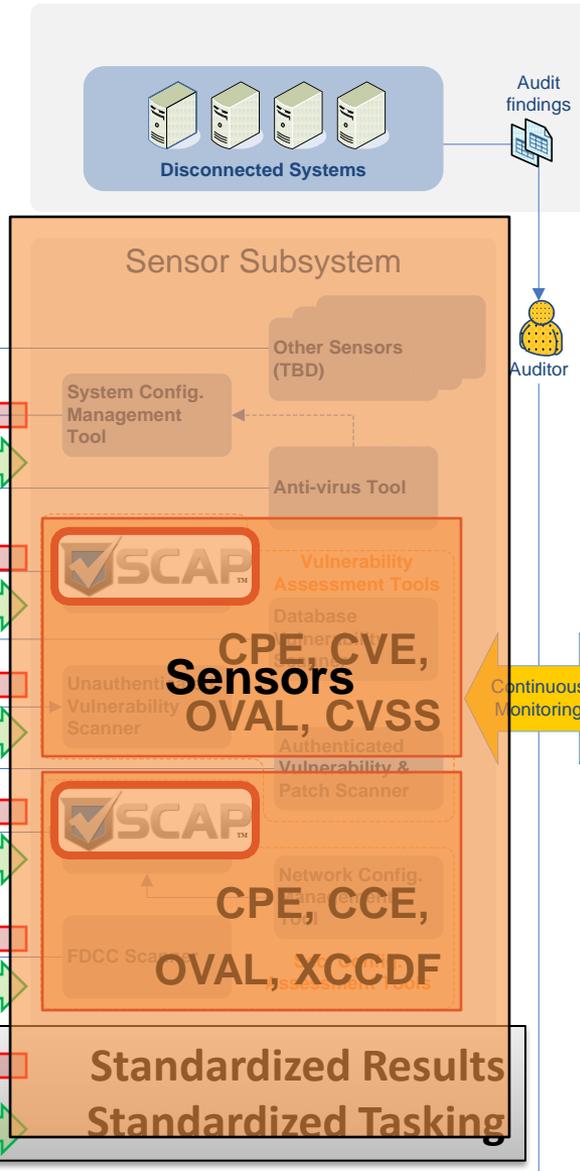
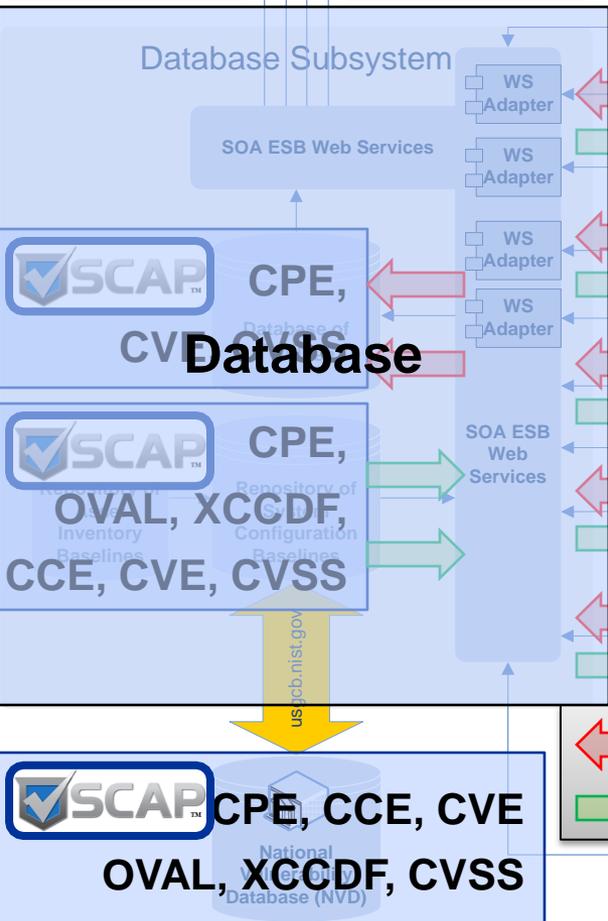
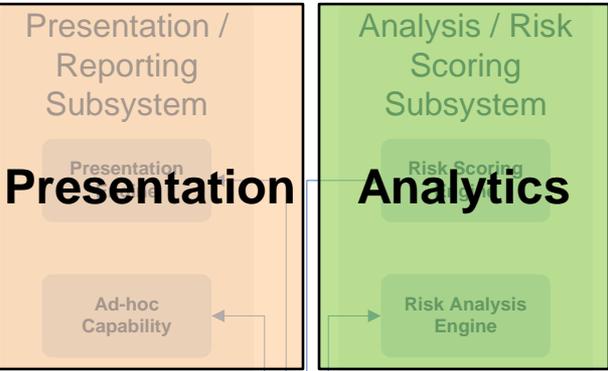
- **CM provides a foundation for many IA activities:**

- FISMA Reporting, Vulnerability Management, Inventory Management, etc.

*“Agencies need to be able to **continuously monitor security-related information from across the enterprise in a manageable and actionable way**. Chief Information Officers (CIOs), Chief Information Security Officers (CISOs), and other agency management all need to have different levels of this information presented to them in ways that enable timely decision making. To do this, **agencies need to automate security-related activities**, to the extent possible, and acquire tools that correlate and analyze security-related information. Agencies need to develop automated risk models and apply them to the vulnerabilities and threats identified by security management tools.”* OMB memo M-10-15

# CAESARS & Standards

CAESARS: Continuous Asset Evaluation, Situational Awareness, and Risk Scoring - Reference Architecture

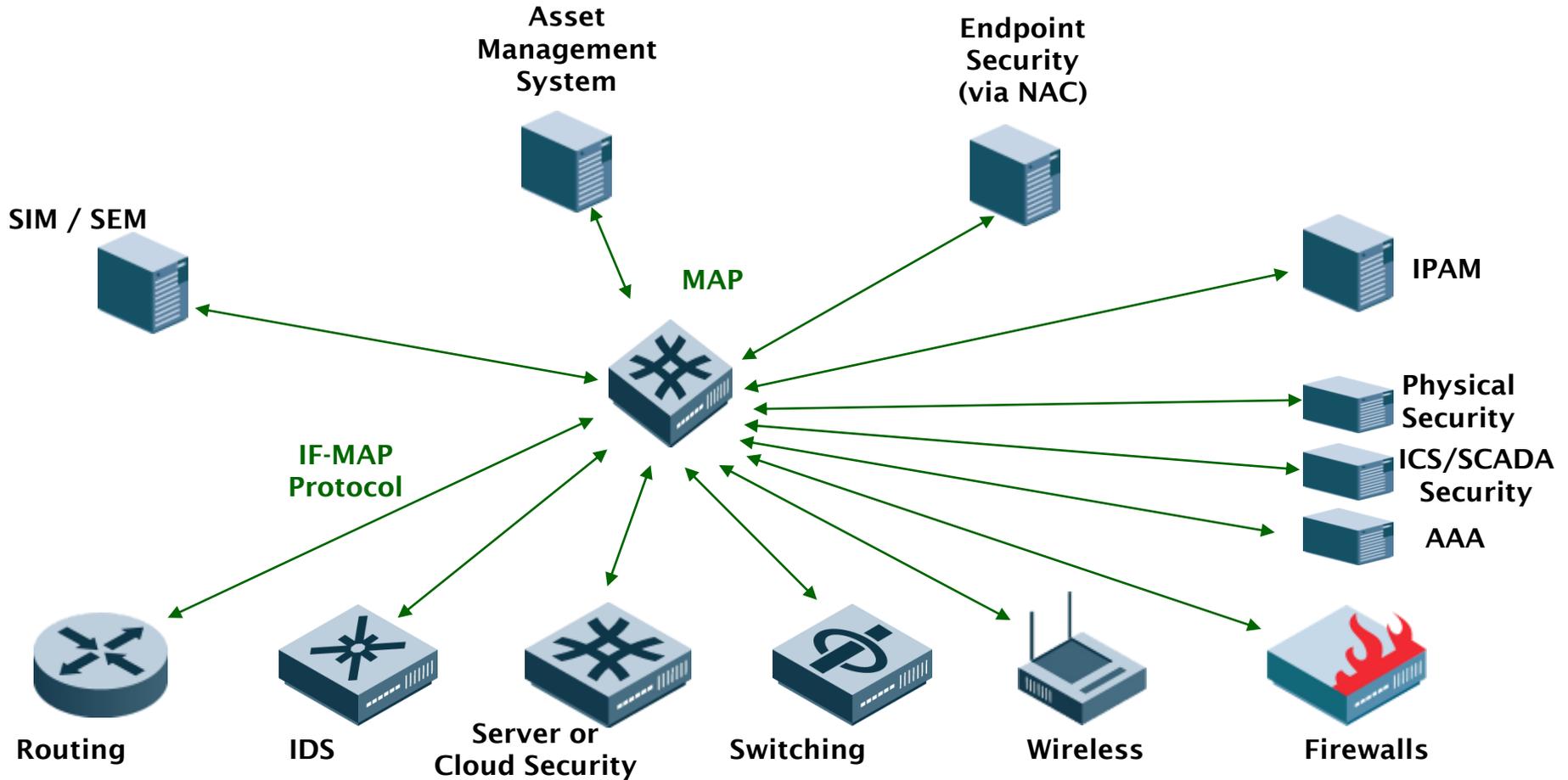


<http://www.dhs.gov/xlibrary/assets/fns-caesars.pdf>

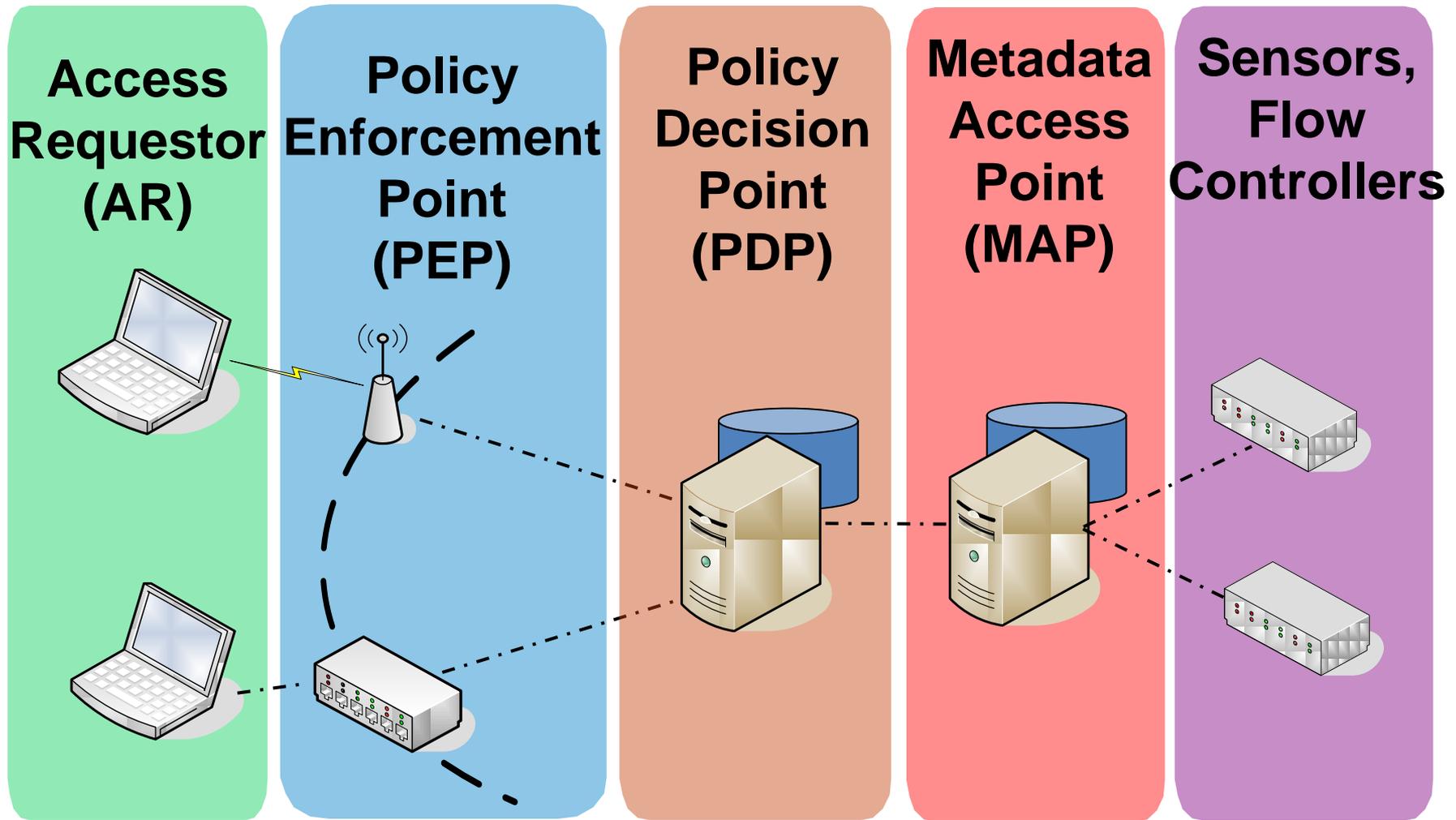
# SCAP and TNC Integration

- **Network Access Control (NAC) is seen as a key enabling technology for several of the SANS Top 20 Critical Security Controls.**
- **SCAP provides a set of standard data formats that can be used to describe desired system configurations.**
- **Trusted Network Connect (TNC) provides a standards based NAC solution.**
  - Enables Coordinated Security
- **SCAP and TNC can be used together to provide a complete standards based approach.**

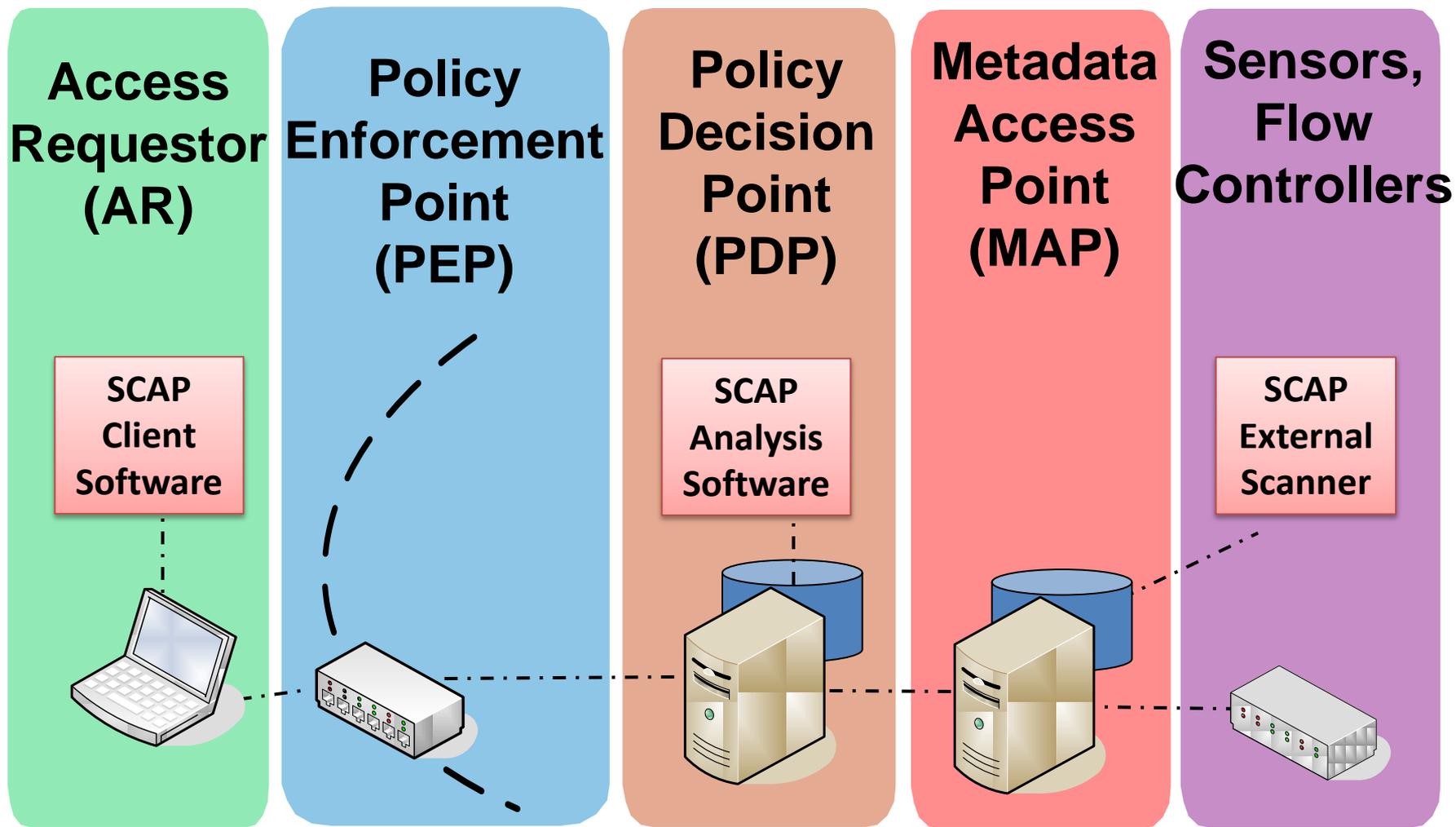
# Coordinated Security



# Coordinated Security & NAC Together



# TNC and SCAP Together



# Standards Enable Broad Interoperability & Flexibility

## ■ Government

- Doesn't use a single solution, but defines broad policy.
- Requires a standard format for expressing the policy.

## ■ Large federated enterprises

- Don't deploy single solutions, but must comply with policy.
- Requires tools that speak in common terms and understand standard policy formats.

## ■ Structured data enables further innovation

- Opportunities for enhanced correlation to drive analytics & response
- Sharing structured actionable information across organizations

# Questions?

# Additional Resources

## ■ Making Security Measurable

- A Collection of Information Security Community Standardization Activities and Initiatives  
<https://msm.mitre.org/> & <https://msm.mitre.org/incubator/>

## ■ SCAP (<http://scap.nist.gov/>)

- Guide to Adopting and Using the Security Content Automation Protocol (SCAP) Version 1.0 (<http://csrc.nist.gov/publications/nistpubs/800-117/sp800-117.pdf>)
- The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.0 (<http://csrc.nist.gov/publications/nistpubs/800-126/sp800-126.pdf>)

## ■ SCAP Component Standards

- CCE – <https://cce.mitre.org/>
- CPE – <https://cpe.mitre.org/>
- CVE – <https://cve.mitre.org/>
- XCCDF – <http://scap.nist.gov/specifications/xccdf/>
- OVAL – <https://oval.mitre.org/>
- OCIL – <http://scap.nist.gov/specifications/ocil/>
- CVSS – <http://www.first.org/cvss/>

## ■ Enterprise Reporting

- AI – <http://csrc.nist.gov/publications/PubsDrafts.html#NIST-IR-7693>
- ARF – <http://csrc.nist.gov/publications/PubsDrafts.html#NIST-IR-7694>

## ■ 2011 Chief Information Officer Federal Information Security Management Act Reporting Metrics

- <http://www.sans.org/critical-security-controls/fisma.pdf>

## ■ DHS Publication: “Enabling Distributed Security in Cyberspace”

- <http://www.dhs.gov/xlibrary/assets/nppd-cyber-ecosystem-white-paper-03-23-2011.pdf>