



# CND Data Strategy and Security Configuration Management

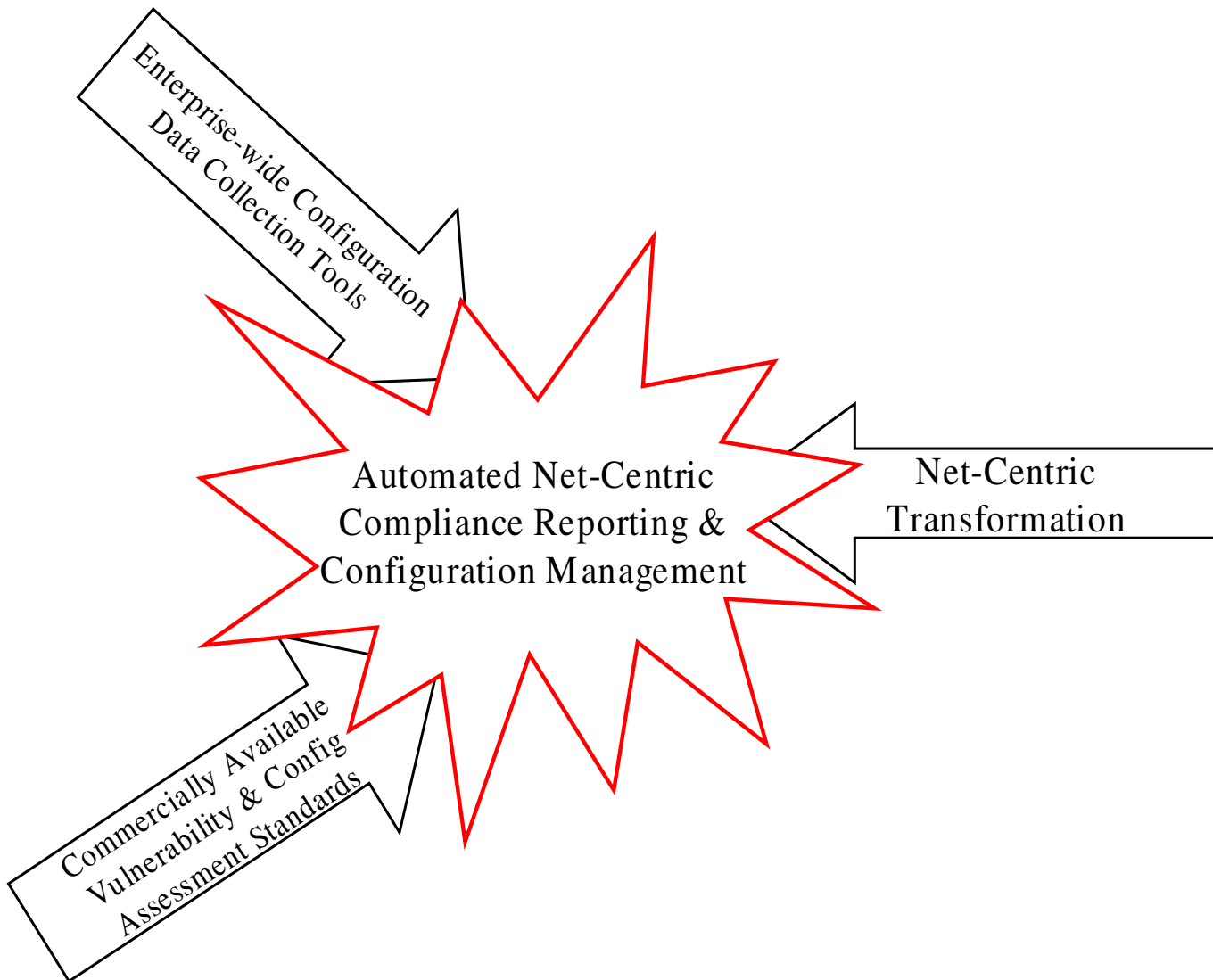
SEP 2008





# Agenda

- CND Data Strategy Pilot
- Build to Architecture/Projects





## Some SCAP Uses



- Vulnerability assessments (OVAL/CVE)
- Assess IAVA (patch) compliance (OVAL)
- Validate host level CTO implementation (OVAL/CCE/CPE)
- Search for artifacts indicating malicious activity (XCCDF/OVAL)
- Collect software inventories (CPE)
- Perform automated C&A validation (XCCDF/OVAL/CCE/CPE)
- Verify correct application of security checklists (XCCDF/OVAL/CCE/CPE)
- Assess user permissions and roles (XCCDF/OVAL)



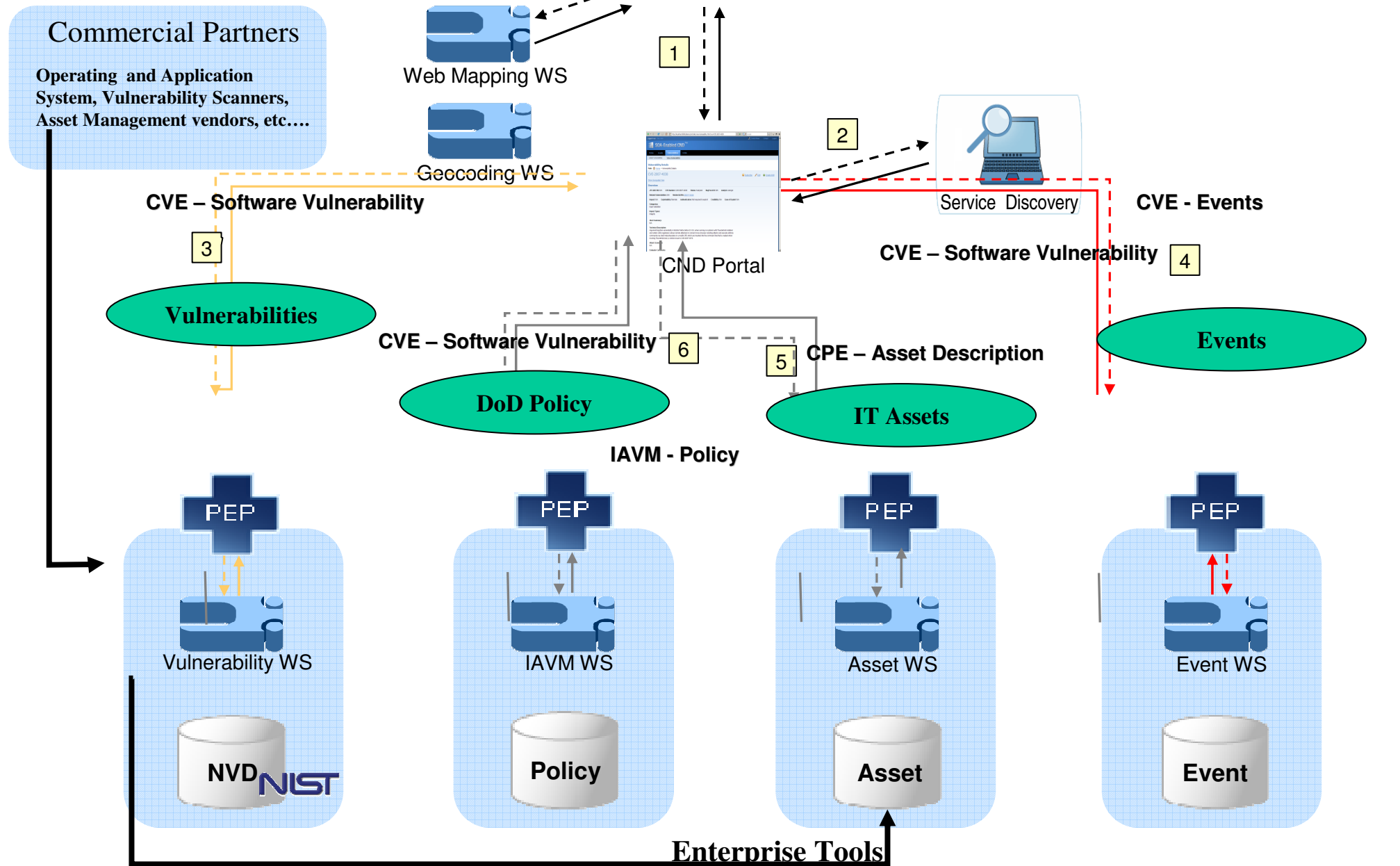
# CND Data Strategy Pilot



# CND Data Strategy Pilot Phase I & II



- Phase I of the CND Pilot will provide a DoD Service Oriented Architecture that enables the correlation of Asset data, Event data, DoD Policy and Security Content Automation Program (SCAP) vulnerability data.
- Phase II of the CND Pilot will add Incident, Certification and Accreditation information, Enterprise Service Management functionality, transition to select Net Centric Enterprise Services functionality, and incorporate additional asset, vulnerability, Event data.





# User Interface



## Notional Data

Logged in as: Doe, John Control Panel Contact Logout


### SOA-Enabled CND <sup>Pilot</sup>

Home Assets Vulnerabilities IAVMs

Assets Summary My Assets

#### My Assets

Path: Home > My Assets



**What type of vulnerabilities?**

**How many assets affected?**

**Where are they located?**

**What patches and guidance are available?**

	IP Address	MAC Address	AOR	MAC	Owner	State	Country
[-]	50.121.210.123	0b:00:00:00:00:01	USNORTHCOM	1	Unit Number 115	Georgia	USA
	<b>Potentially Vulnerable To:</b> <a href="#">CVE-2005-2090</a> <a href="#">CVE-2005-4836</a> <a href="#">CVE-2007-1355</a> <a href="#">CVE-2007-2450</a> <a href="#">CVE-2007-3074</a> <a href="#">CVE-2007-3089</a> <a href="#">CVE-2007-3090</a> <a href="#">CVE-2007-3285</a> <a href="#">CVE-2007-3382</a> <a href="#">CVE-2007-3383</a> <a href="#">CVE-2007-3385</a> <a href="#">CVE-2007-3511</a> <a href="#">CVE-2007-3657</a> <a href="#">CVE-2007-3734</a> <a href="#">CVE-2007-3735</a> <a href="#">CVE-2007-3736</a> <a href="#">CVE-2007-3737</a> <a href="#">CVE-2007-3738</a> <a href="#">CVE-2007-4038</a>						
[-]	50.121.202.7	00:F0:8b:8A:fc:2f	USNORTHCOM	2	Unit Number 115	Georgia	USA
	<b>Potentially Vulnerable To:</b> None						
[-]	50.121.202.50	08:00:20:BE:3C:90	USNORTHCOM	3	Unit Number 115	Georgia	USA
	<b>Potentially Vulnerable To:</b> <a href="#">CVE-2005-2090</a> <a href="#">CVE-2005-4836</a> <a href="#">CVE-2007-1355</a> <a href="#">CVE-2007-2450</a> <a href="#">CVE-2007-3382</a> <a href="#">CVE-2007-3383</a> <a href="#">CVE-2007-3385</a>						
[+]	50.121.202.1	00:01:ba:5D:94:43	USNORTHCOM	3	Unit Number 115	Georgia	USA
[+]	50.121.202.2	00:01:ba:5D:94:43	USNORTHCOM	3	Unit Number 115	Georgia	USA



# SCAP Evolution

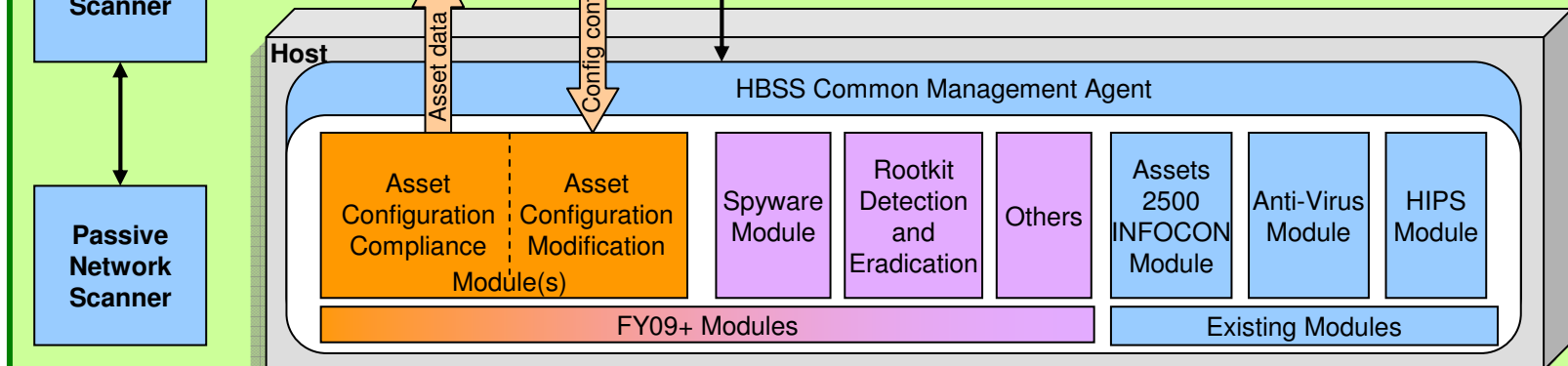
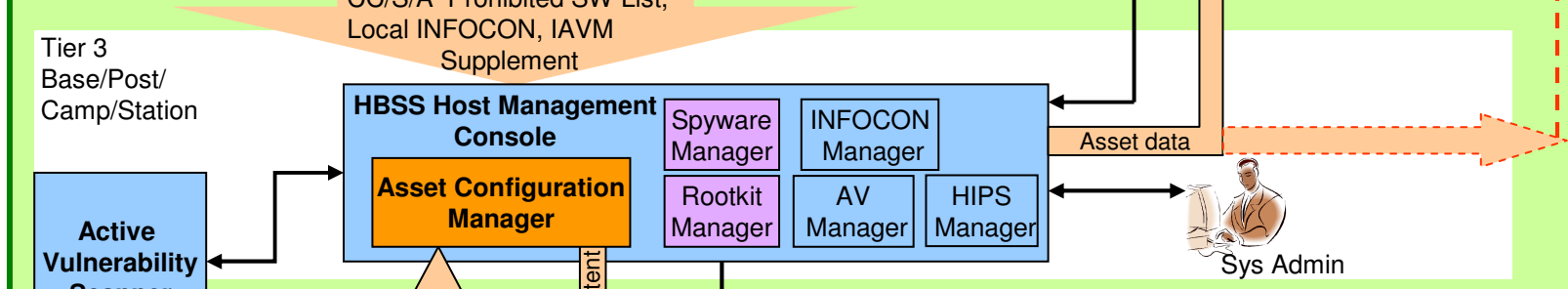
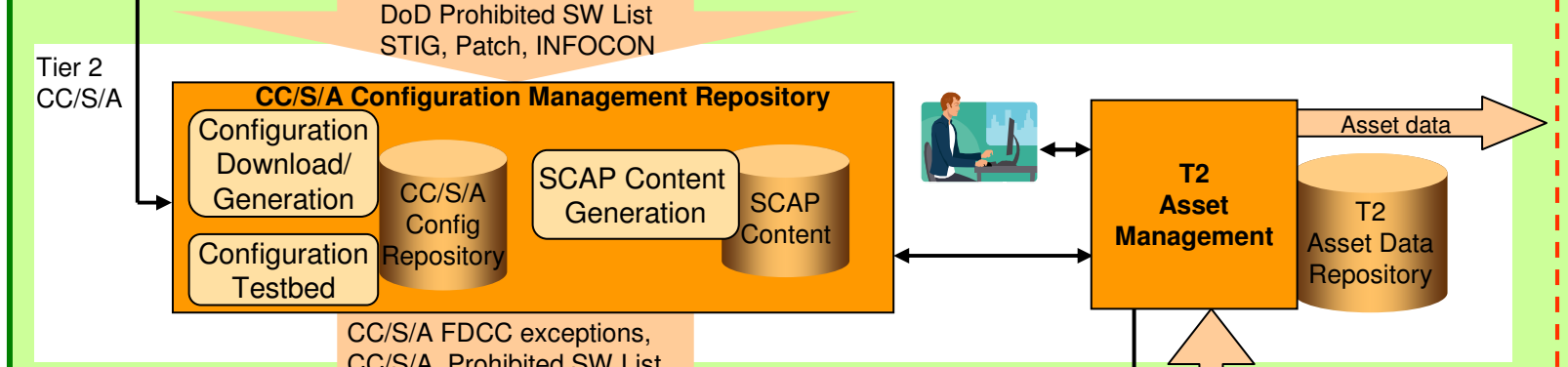
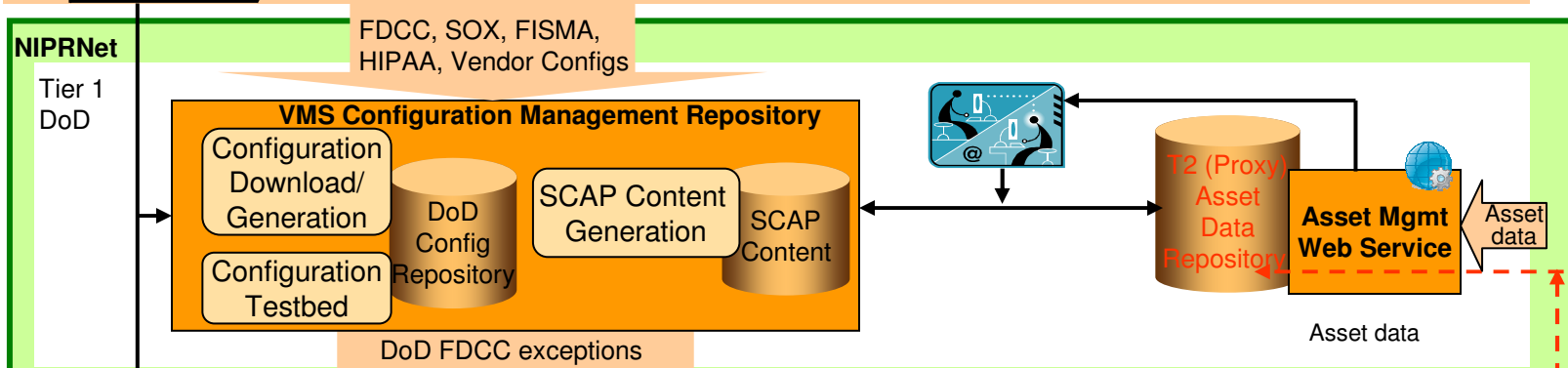
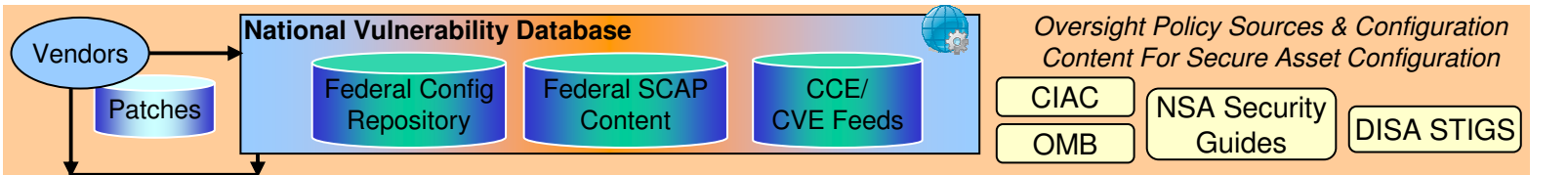


- Fill gaps in existing SCAP CM standards
  - Remediation language – link weak configurations & vulnerabilities to standard remedies
  - SCAP interfaces – automate assessment policies & results sharing between SCAP tools
- Expand into AS&W and Risk Management
  - Event and Incident sharing standards
  - Network & Risk standards





# Build-to Architecture/Projects



**Enhanced Configuration Management and Computer Network Defense**

- CM Capability
- CND Capability To Be Developed Under Other initiatives
- Existing Capability

# National Vulnerability Database (NVD) Redesign NIST

SCAP Standards Development

Vulnerability Management System (VMS) Redesign  
DISA

SCAP Standards Development  
MITRE/NSA

IAVM  
Business  
Process  
Re-  
engineering  
ASD/NII

SCAP  
Standards  
Development  
MITRE/NSA

Asset Data  
Repository  
Development  
DISA

CND UDOP  
Enterprise  
Service Bus  
(ESB)/  
Cross  
Domain  
Solution  
(CDS)  
DISA

Asset Data  
Repository  
Development  
DISA

SCAP Standards Development  
MITRE/NSA

SCCVI  
Recompete  
ESSG

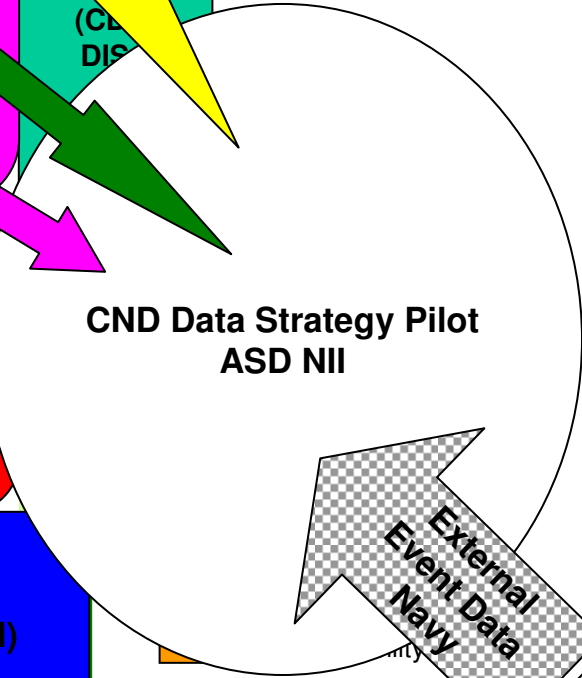
SCAP  
Standards  
Development  
MITRE/NSA

Small Agency Pilot  
NSA/ASD NII

Asset Configuration Compliance Module (ACCM)  
Enterprise Solutions Steering Group (ESSG)



QDR  
Trickler  
DISA/NSA

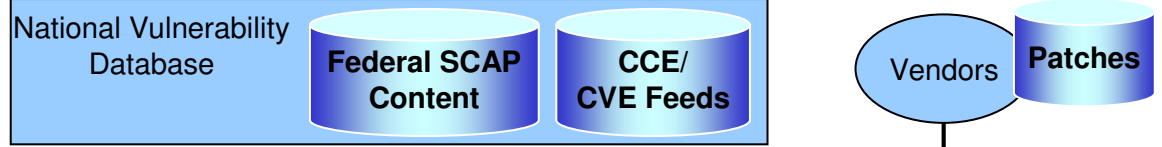
SCAP Standards  
Development  
MITRE/NSA



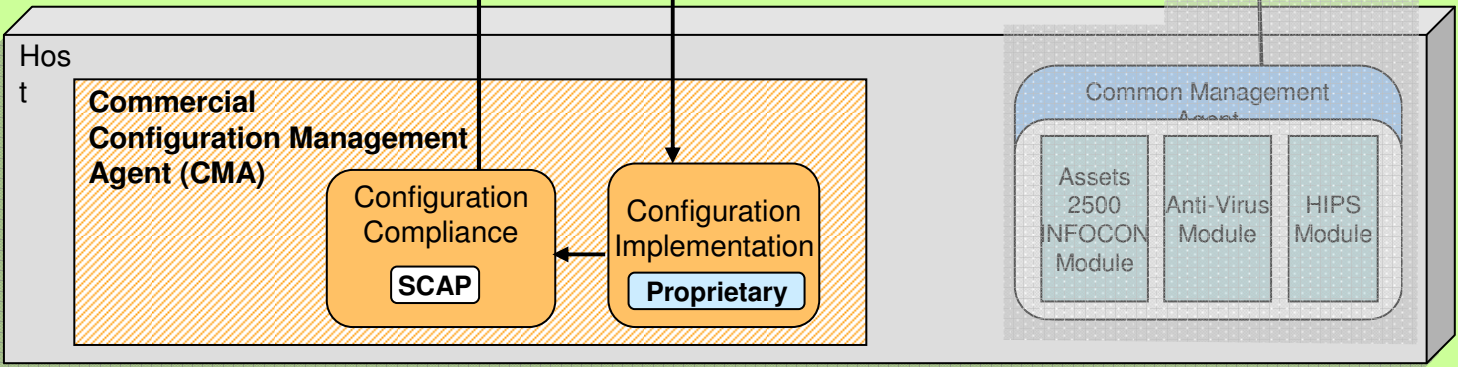
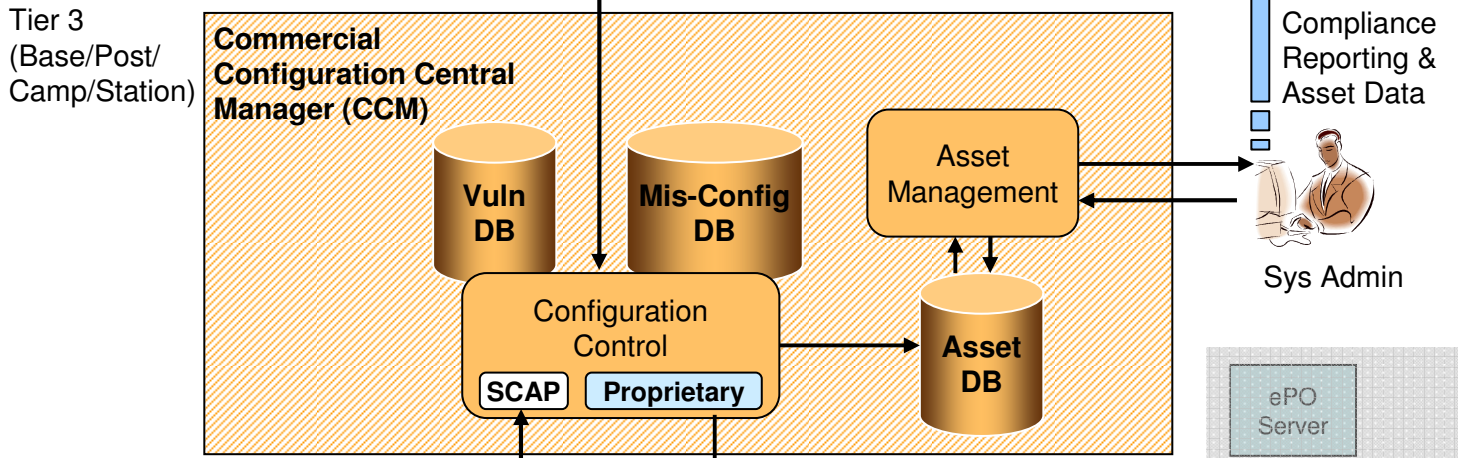
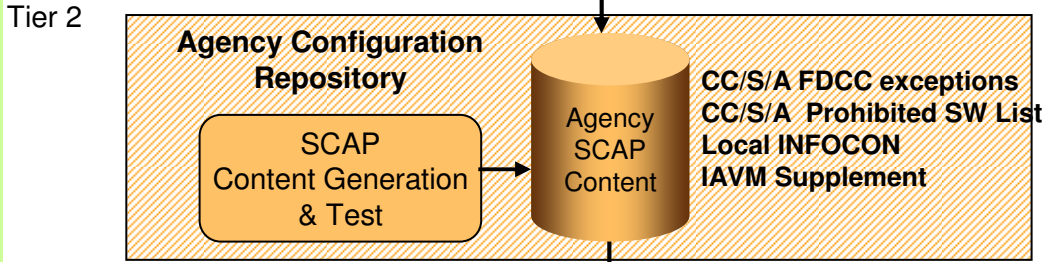
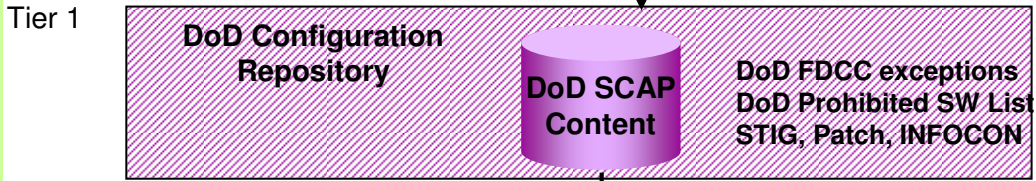
CND Data Strategy Pilot  
ASD NII

External  
Event Data  
Navy




-  CND Capability To Developed Under Other initiatives
-  Existing Capability

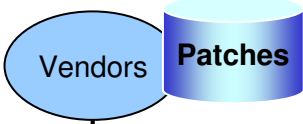


**NIPRNet**

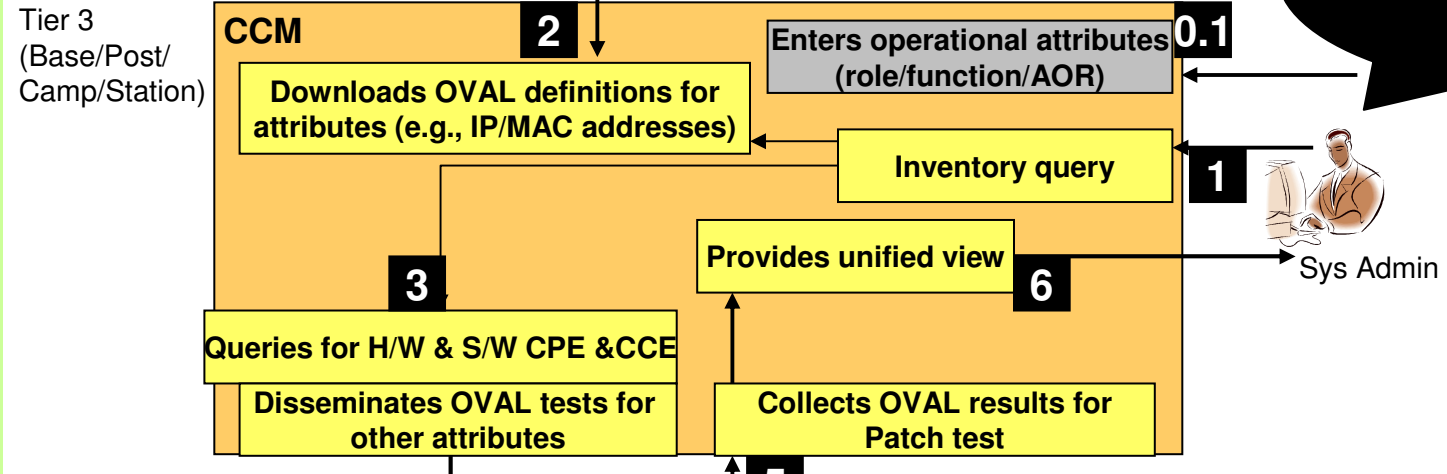
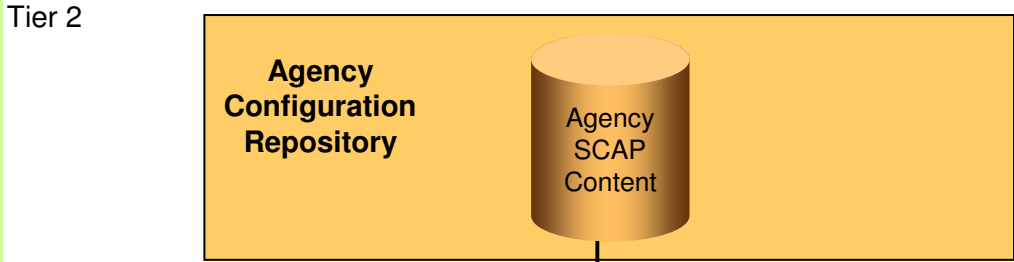
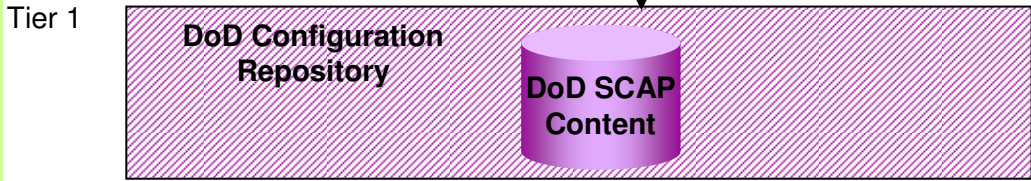


**Configuration Management  
SCAP Small Agency  
Scope  
Spiral 1 Increment 1**

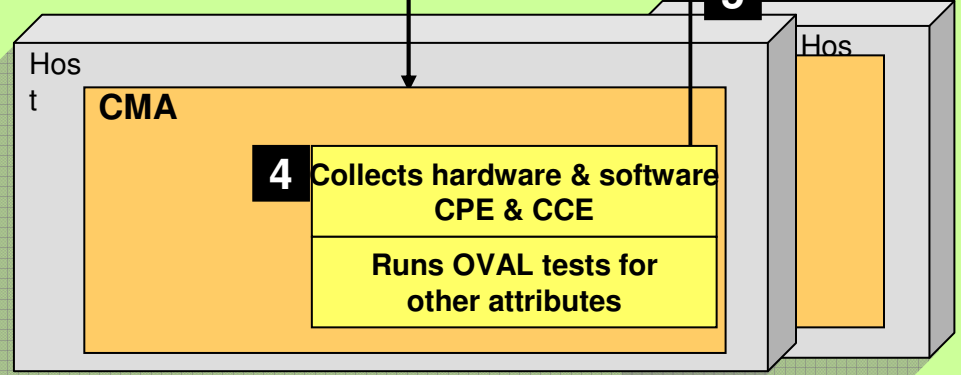
-  Pilot Capability
-  Capability To Be Developed Under Other initiatives
-  Existing Capability

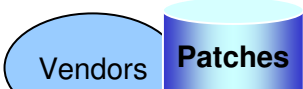
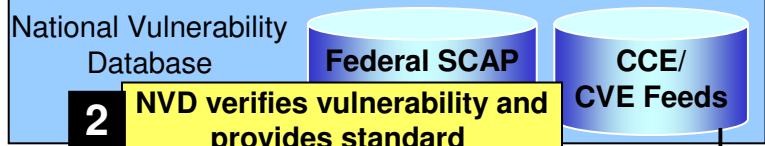


**NIPRNet**



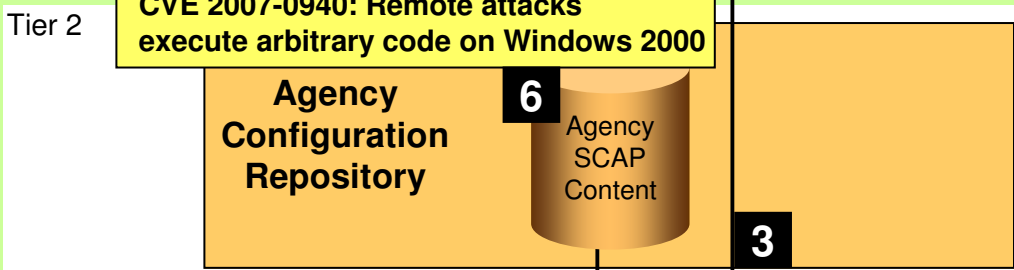
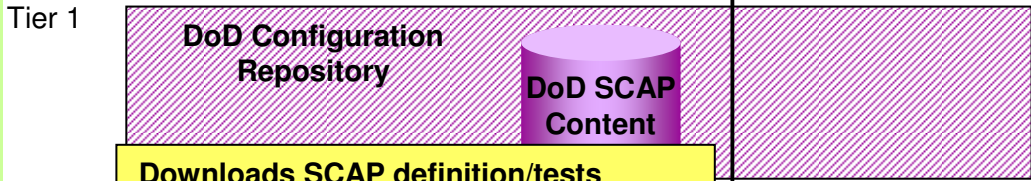
What is my hardware and software inventory?



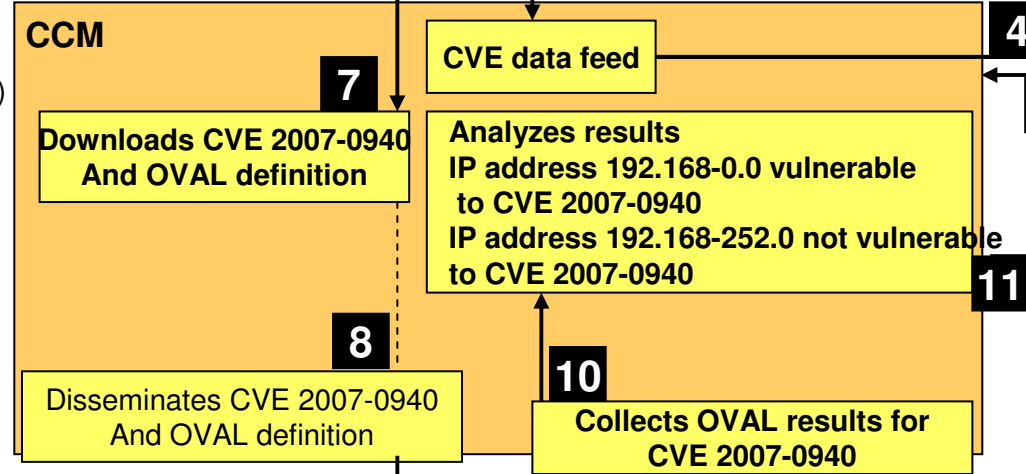


**1** New Microsoft Windows 2000 Vulnerability discovered

NIPRNet



Tier 3 (Base/Post/Camp/Station)

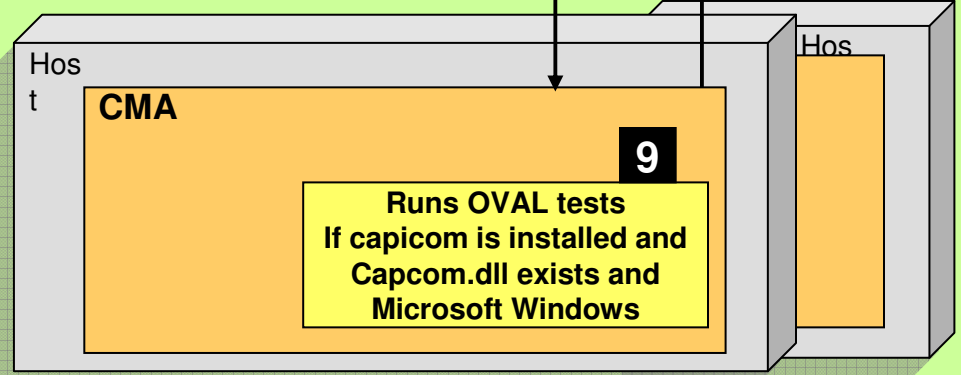


How many of the Agency's 100 boxes are impacted by this new vulnerability?



Sys Admin

44 boxes



**2**

**1**

**6**

**3**

**7**

**4**

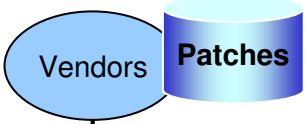
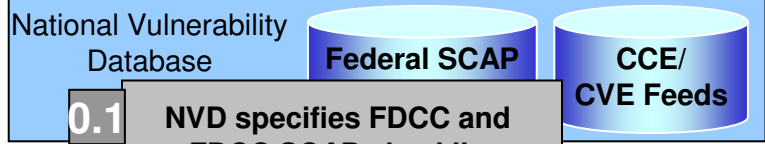
**5**

**11**

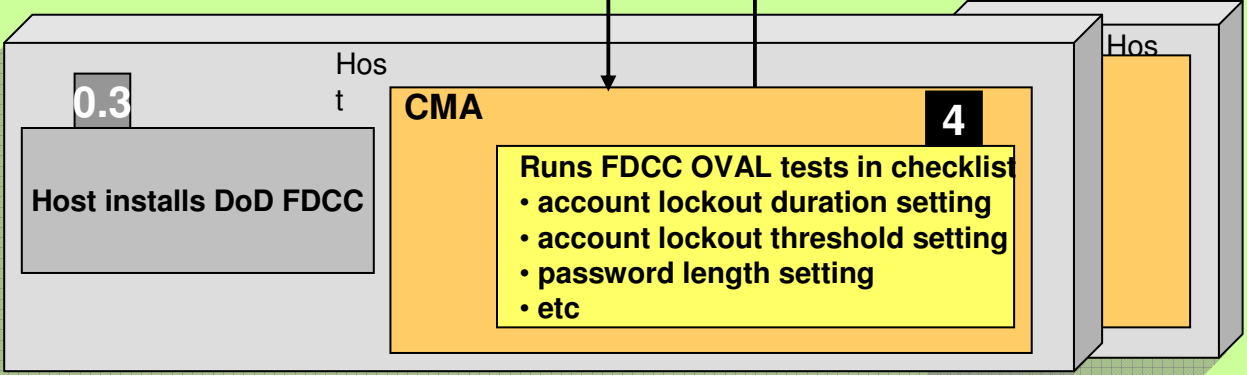
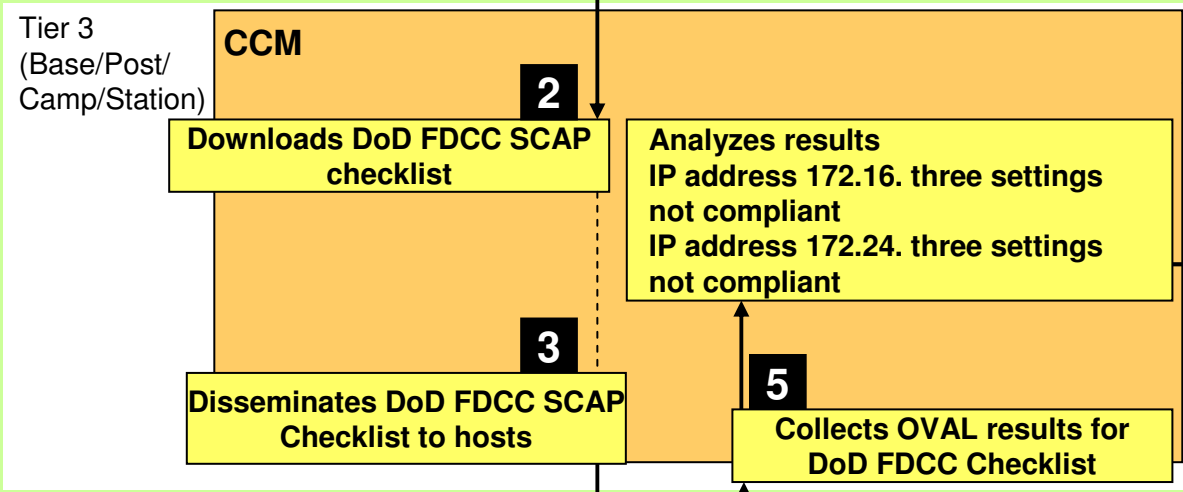
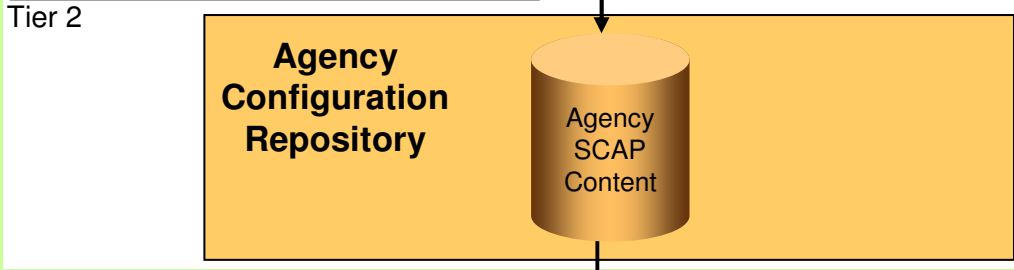
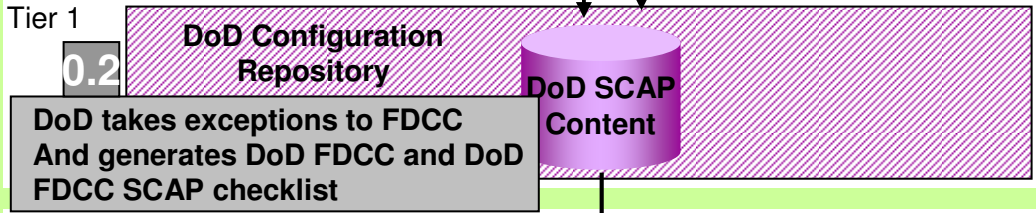
**8**

**10**

**9**

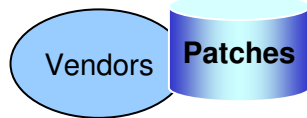


**NIPRNet**



Are my Agency's 100 boxes still compliant with the DoD FDCC installed last week?



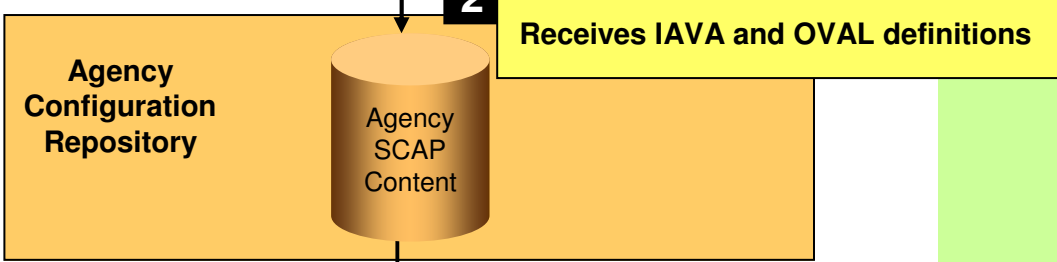


**NIPRNet**

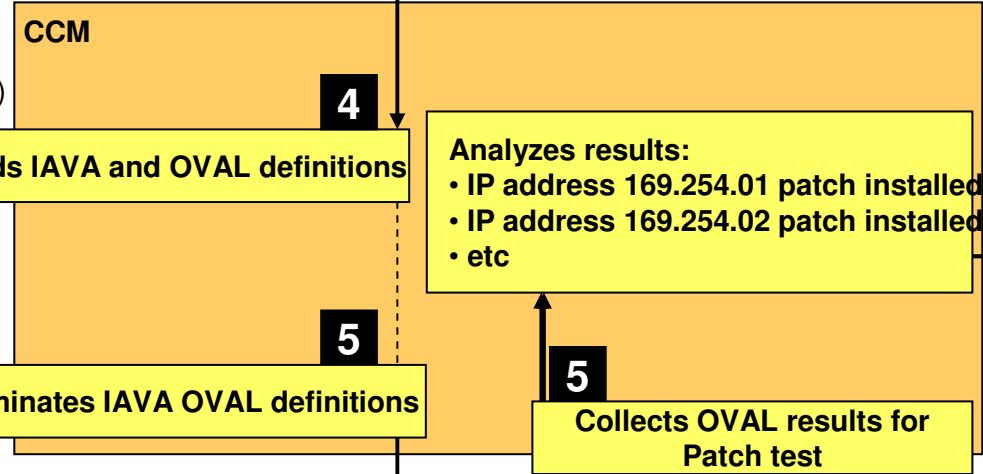
Tier 1



Tier 2



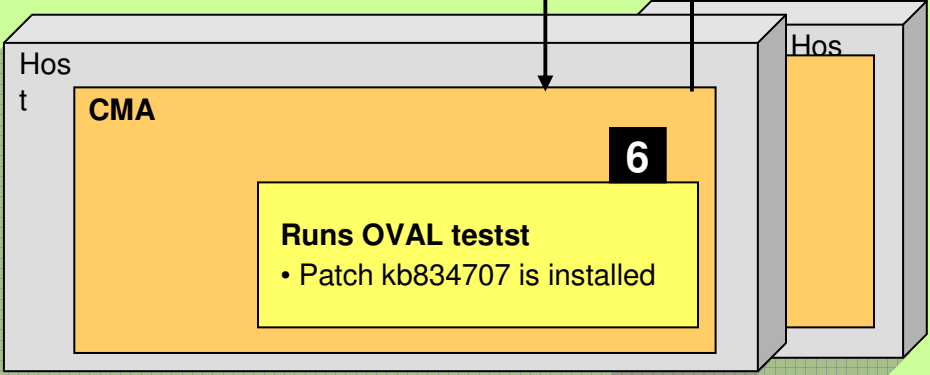
Tier 3  
(Base/Post/  
Camp/Station)



Are the Agency's 100 boxes compliant with all applicable IAVAs?



**8** Sys Admin **All boxes IAVA compliant**







# Summary



- Combining data strategy and configuration management infrastructure to build an enterprise capability
  - Convert existing content and standards to machine readable format
  - Build local, component, and enterprise SA security configuration
  - Standards-based to support scalability and vendor neutrality in the future



# Backup Slides



# Federal/Industry Baseline Config Policy Audit

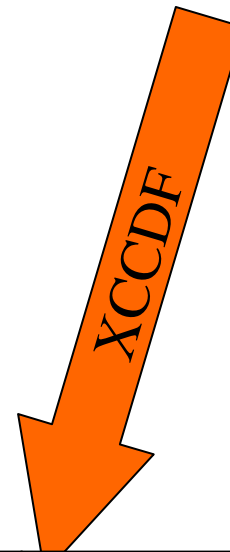
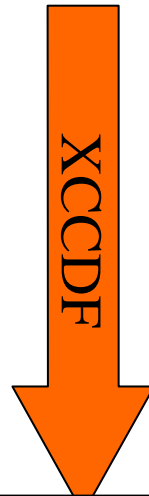
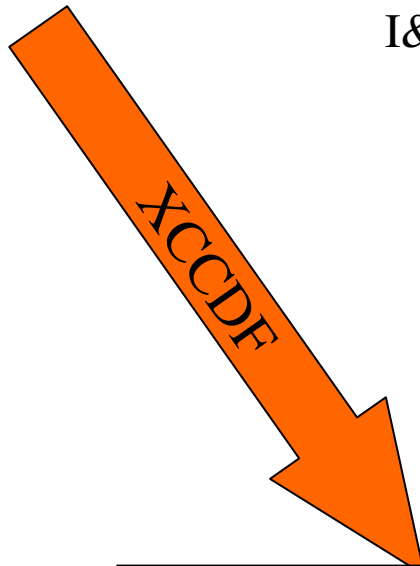
FDCC  
FISMA  
HIPAA  
SOX  
Vendor Configs  
Other best practice

# DoD Configuration Policy Audit

IAVM  
CTO  
STIG  
DoD FDCC exceptions  
Patch  
DoD Allowed/Prohibited SW List  
INFOCON  
I&W Collection

# CC/S/A Configuration Policy Audit

Enterprise Licensing  
Local INFOCON  
CC/S/A FDCC exceptions  
IAVM Supplements  
IAVM Exceptions  
CC/S/A Allowed/Prohibited SW List



# Comprehensive Audit Policy

- OVAL
- CPE
- CVE
- CCI
- CCE