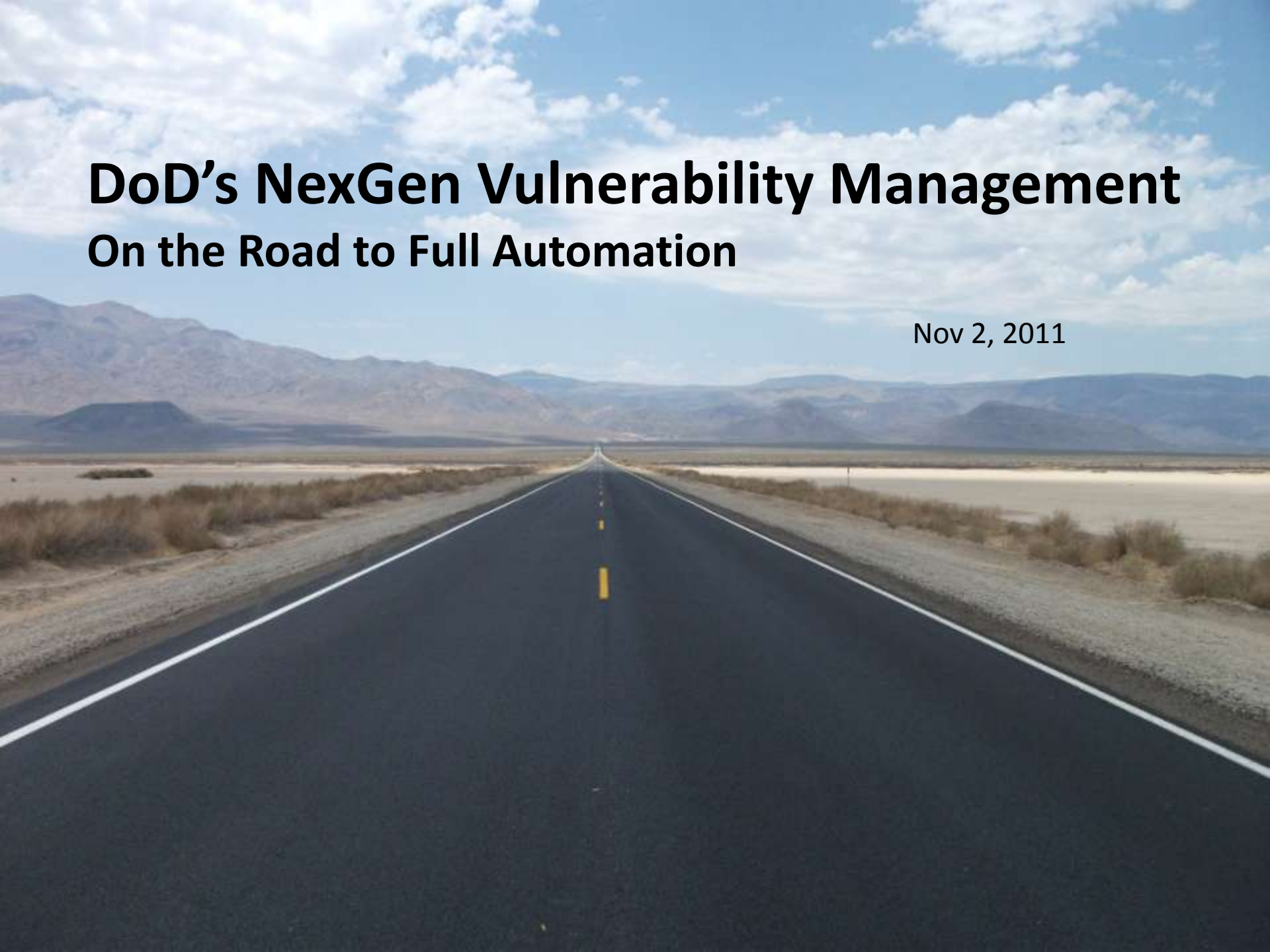


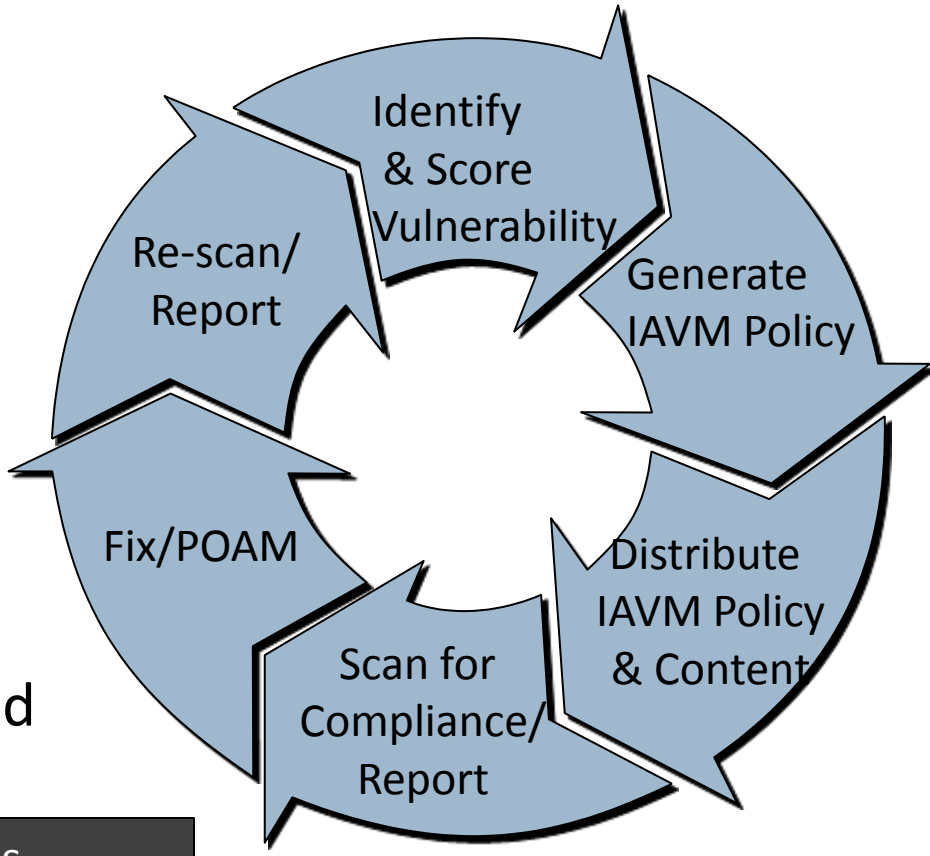
DoD's NexGen Vulnerability Management

On the Road to Full Automation

Nov 2, 2011

We know that 80%+ of successful Cyber attacks are related to known vulnerabilities and misconfigurations however…

- DoD process for scoring vulnerabilities is subjective
- IAVM compliance reporting procedures are manual, resource intensive, slow and inaccurate
- DoD systems for tracking vulnerability compliance are siloed and lack standard interfaces



VMS
eEye Retina
eMASS

DoD's first step toward automation – IAVM System 1.0

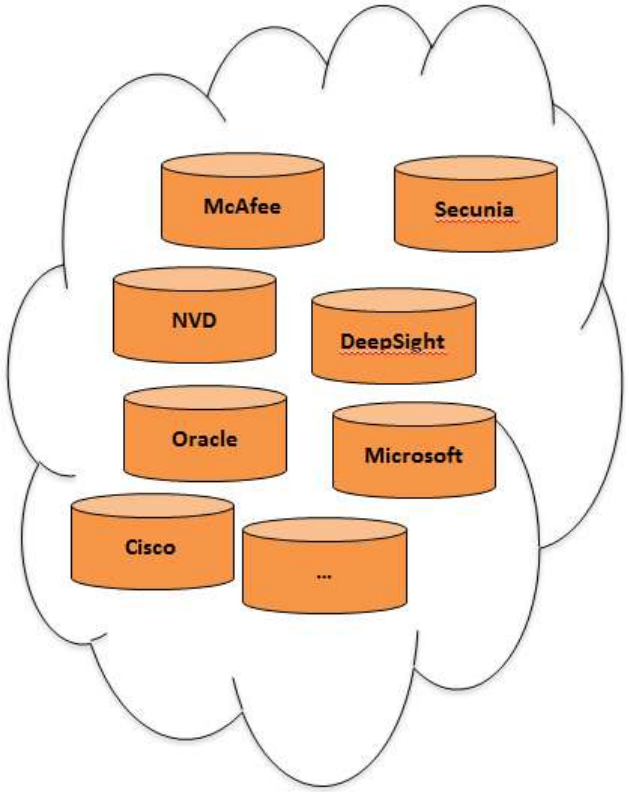
- Automates USCYBERCOM vulnerability scoring process
- Includes CVSS-compliant scoring engine
- Provides real-time interfaces with Symantec DeepSight, NVD, and VMS
- Supports SCAP standards including CVE, CVSS, and CPE

Scheduled Go Live Jan, 2012

Wouldn't it be nice if…

- IAVMs were directly actionable – "apply this patch" or "upgrade this application"
- You could quickly identify your most vulnerable assets
- You could easily determine the priority for patching and remediation actions

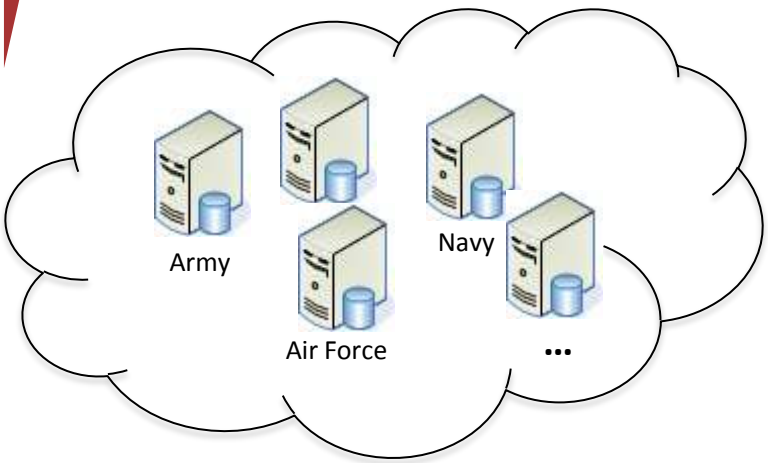
NexGen IAVM will make life easier…



Vulnerability Data Sources

NexGen IAVM

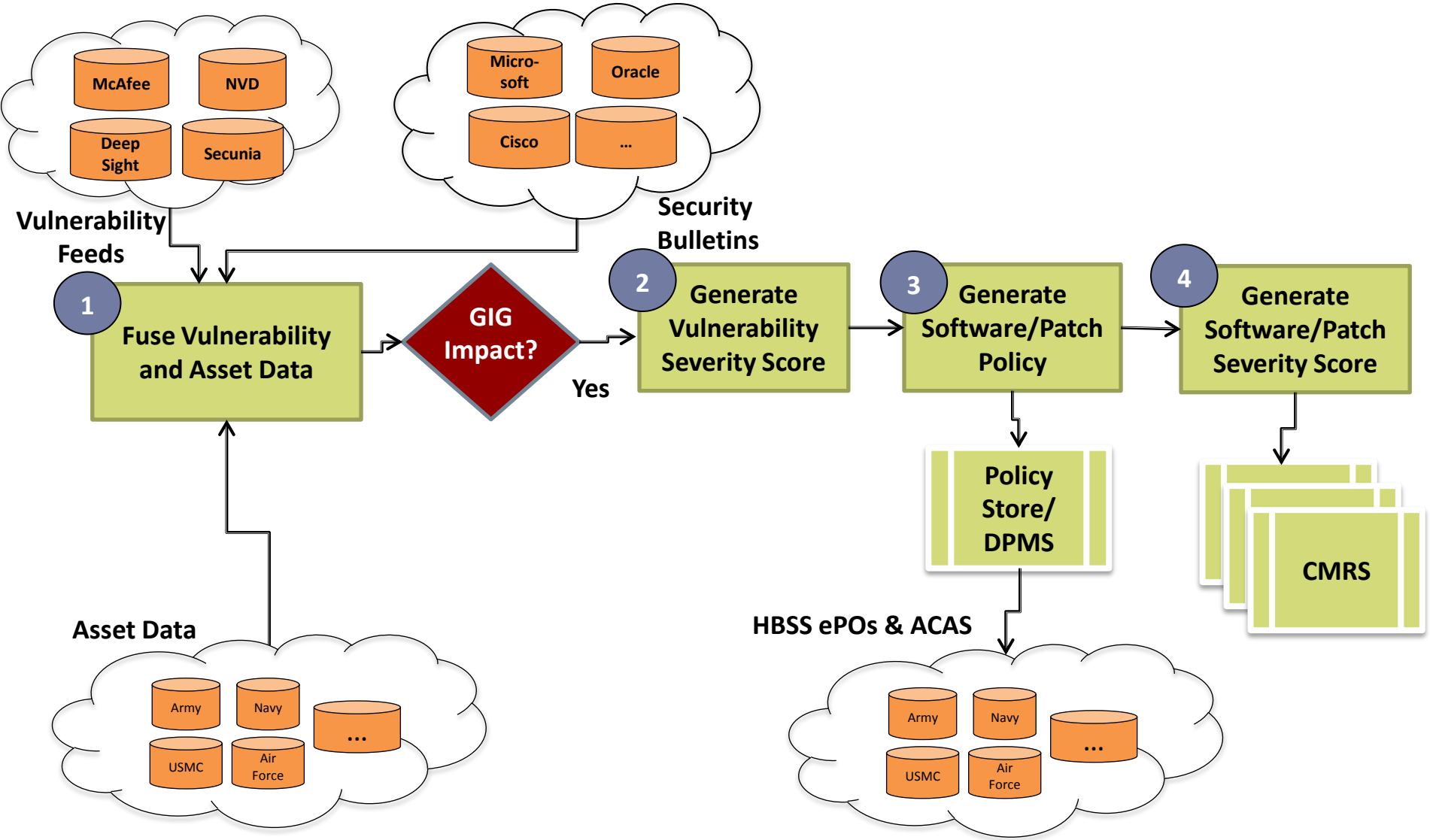
Continuous Monitoring System



DoD Vulnerability Scanners (HBSS/ACAS)

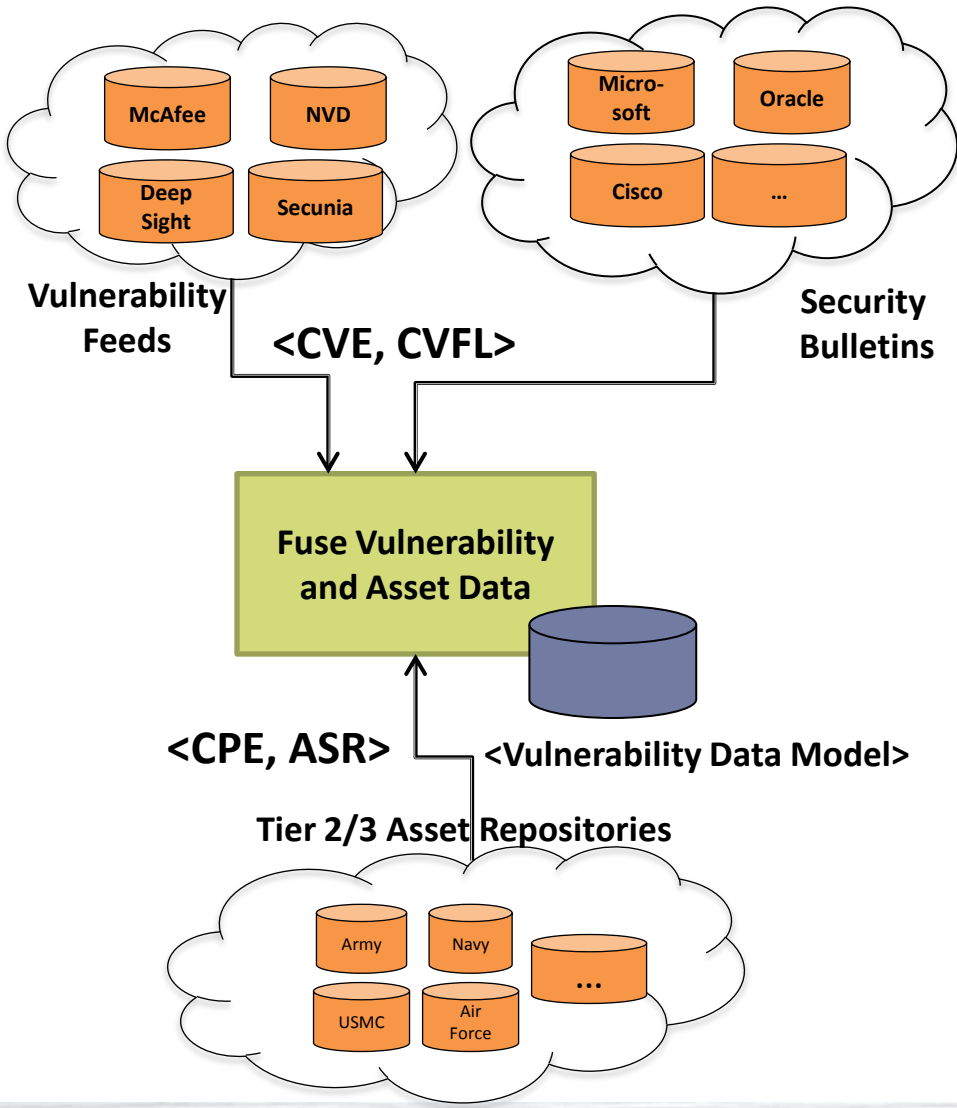
- One IAVM Policy Per Software Platform or Patch
- Automated Compliance Checking
- Prioritized List of Remediation Actions

NexGen IAVM Process Flow – Overview



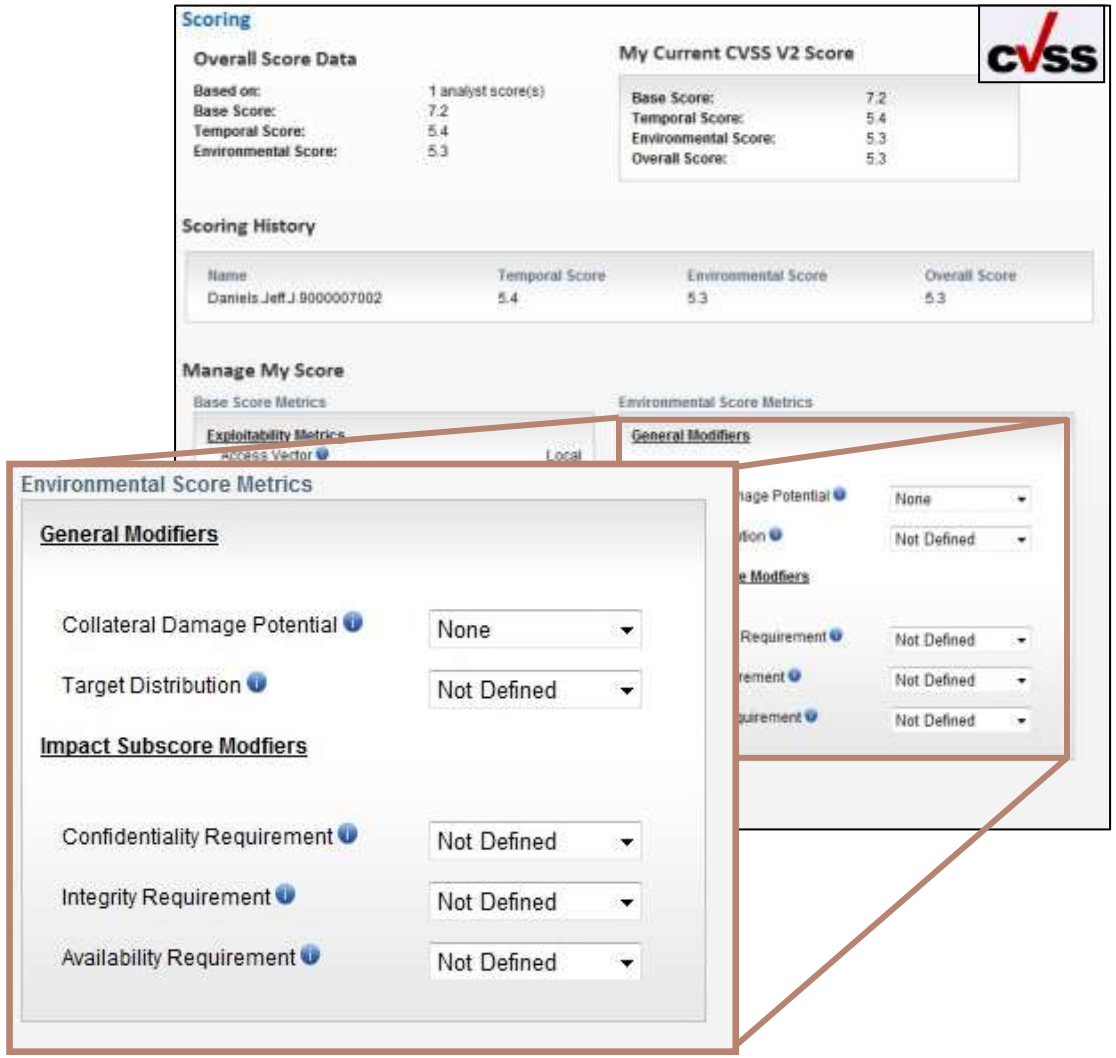
Do I have the latest vulnerability information and how does it impact the GIG?

- Vulnerability info will be aggregated in Common Vulnerability Reporting Format (CVRF) from multiple sources
- Vulnerability info will be processed and stored in standard format - Vulnerability Data Model (VDM)
- GIG-wide software/patch metrics data will be aggregated and correlated with vulnerability data to identify potential impact



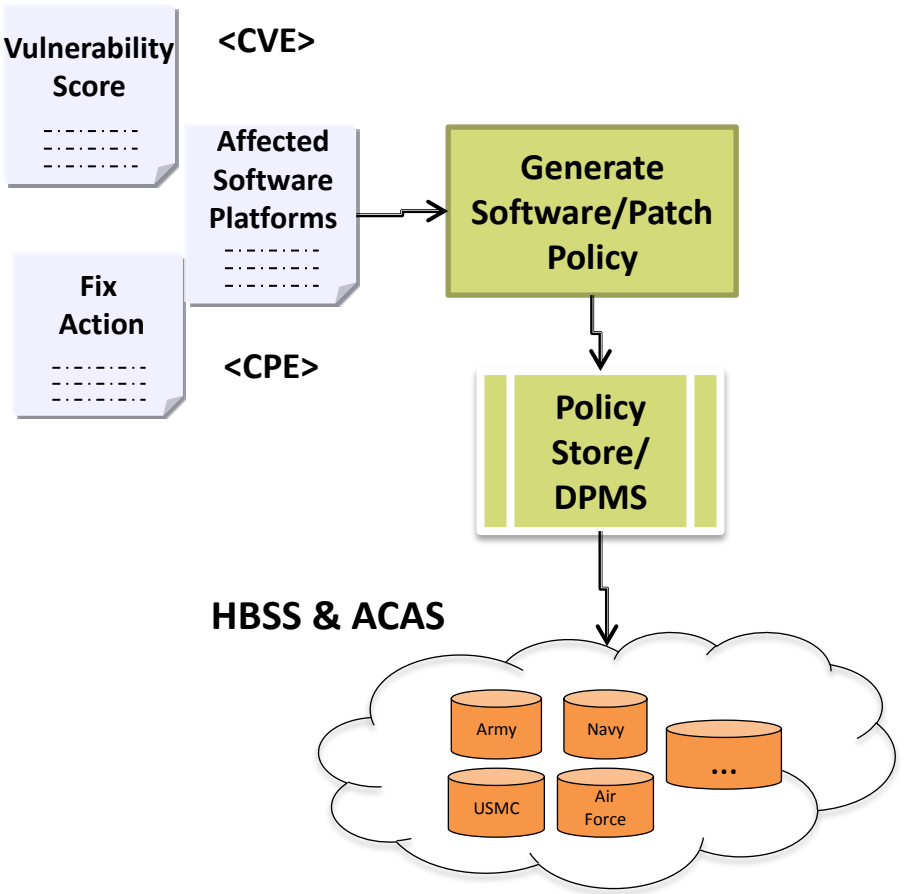
How do I quantify the risk this vulnerability present to the GIG?

- Asset data will be used to auto-populate CVSS target distribution, collateral damage and security metrics
- Analyst will use incident and indicator/event data to populate temporal metrics
- **All** vulnerabilities will be scored if GIG impact identified



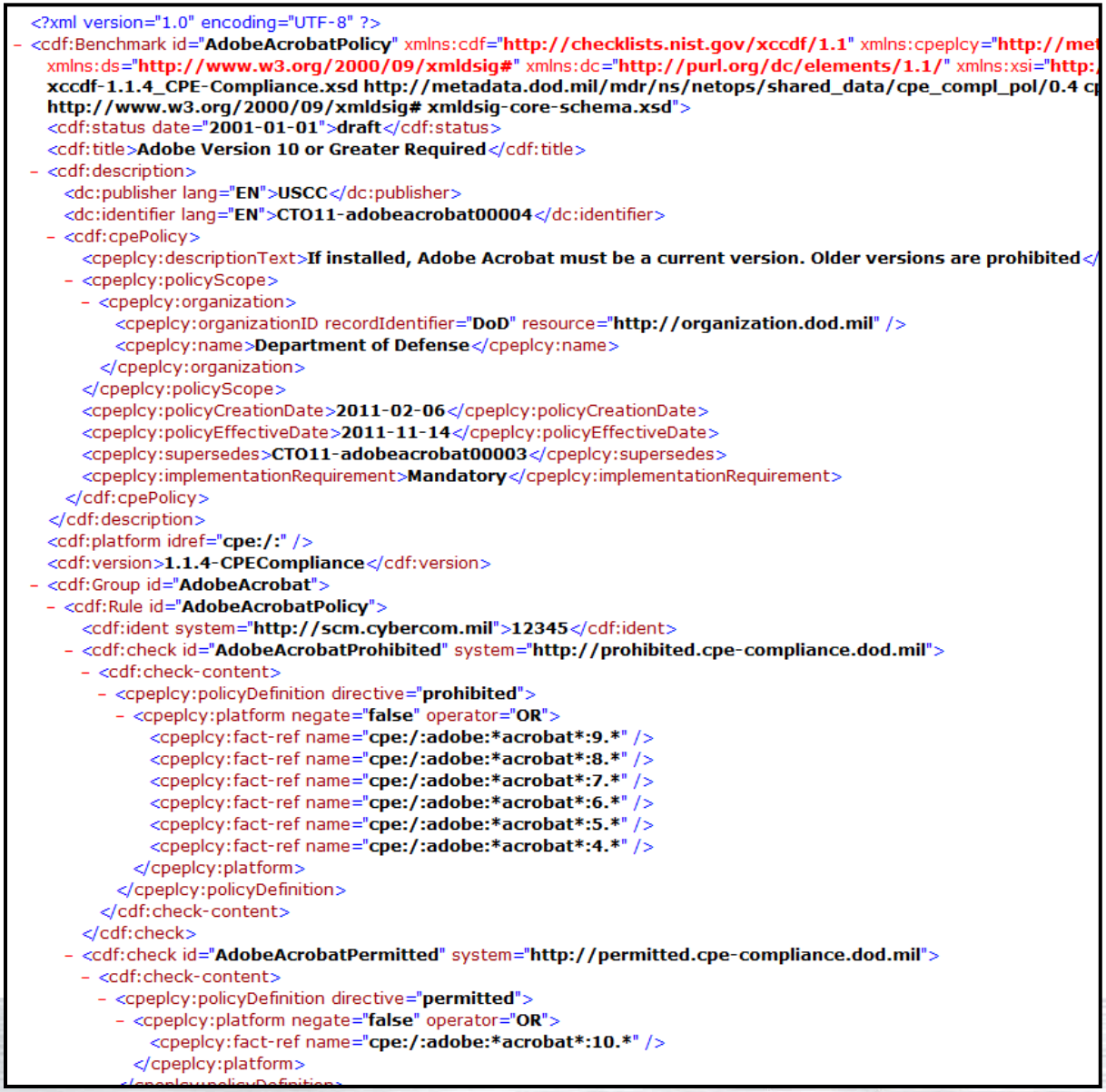
How do I determine by vulnerability posture?

- Vulnerability scores used to generate Platform or Patch specific severity score
- Benchmark content will be **auto-generated** in XCCDF/CPE format and distributed down to host and network scanners
- Most vulnerability compliance scans will be performed at the asset repository level and not on the end points



Platform-based policies will significantly simplify vulnerability management across the DoD

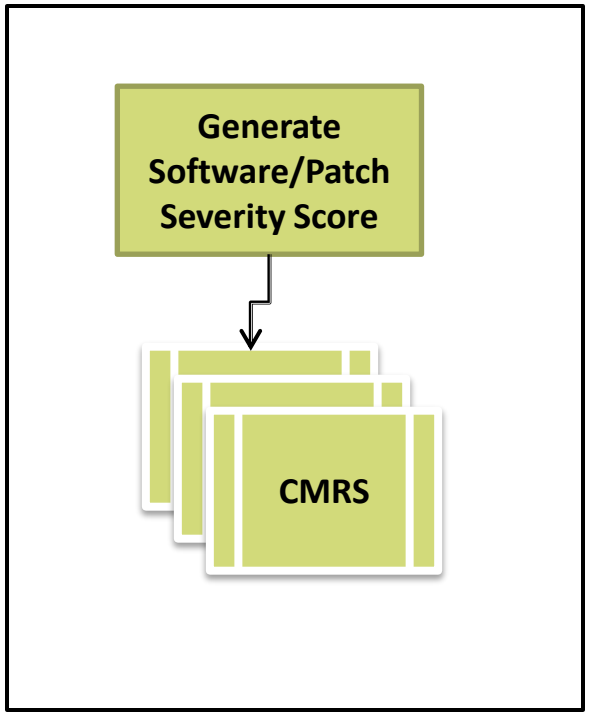
- DOD will have one vulnerability policy per software platform or patch
- Policies will be generated for prohibited, permitted, and required software
- Policies can be run against asset repositories and Host/Network scanners for near real-time results



```
<?xml version="1.0" encoding="UTF-8" ?>
- <cdf:Benchmark id="AdobeAcrobatPolicy" xmlns:cdf="http://checklists.nist.gov/xccdf/1.1" xmlns:cpeplcy="http://me
  xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:dc="http://purl.org/dc/elements/1.1/" xmlns:xsi="http:/
  xccdf-1.1.4_CPE-Compliance.xsd http://metadata.dod.mil/mdr/ns/netops/shared_data/cpe_compl_pol/0.4 cp
  http://www.w3.org/2000/09/xmldsig# xmldsig-core-schema.xsd">
  <cdf:status date="2001-01-01">draft</cdf:status>
  <cdf:title>Adobe Version 10 or Greater Required</cdf:title>
  - <cdf:description>
    <dc:publisher lang="EN">USCC</dc:publisher>
    <dc:identifier lang="EN">CTO11-adobeacrobat00004</dc:identifier>
    - <cdf:cpePolicy>
      <cpeplcy:descriptionText>If installed, Adobe Acrobat must be a current version. Older versions are prohibited</
      - <cpeplcy:policyScope>
        - <cpeplcy:organization>
          <cpeplcy:organizationID recordIdentifier="DoD" resource="http://organization.dod.mil" />
          <cpeplcy:name>Department of Defense</cpeplcy:name>
        </cpeplcy:organization>
      </cpeplcy:policyScope>
      <cpeplcy:policyCreationDate>2011-02-06</cpeplcy:policyCreationDate>
      <cpeplcy:policyEffectiveDate>2011-11-14</cpeplcy:policyEffectiveDate>
      <cpeplcy:supersedes>CTO11-adobeacrobat00003</cpeplcy:supersedes>
      <cpeplcy:implementationRequirement>Mandatory</cpeplcy:implementationRequirement>
    </cdf:cpePolicy>
  </cdf:description>
  <cdf:platform idref="cpe:/:" />
  <cdf:version>1.1.4-CPECompliance</cdf:version>
  - <cdf:Group id="AdobeAcrobat">
    - <cdf:Rule id="AdobeAcrobatPolicy">
      <cdf:ident system="http://scm.cybercom.mil">12345</cdf:ident>
      - <cdf:check id="AdobeAcrobatProhibited" system="http://prohibited.cpe-compliance.dod.mil">
        - <cdf:check-content>
          - <cpeplcy:policyDefinition directive="prohibited">
            - <cpeplcy:platform negate="false" operator="OR">
              <cpeplcy:fact-ref name="cpe:/:adobe:*acrobat*:9.*" />
              <cpeplcy:fact-ref name="cpe:/:adobe:*acrobat*:8.*" />
              <cpeplcy:fact-ref name="cpe:/:adobe:*acrobat*:7.*" />
              <cpeplcy:fact-ref name="cpe:/:adobe:*acrobat*:6.*" />
              <cpeplcy:fact-ref name="cpe:/:adobe:*acrobat*:5.*" />
              <cpeplcy:fact-ref name="cpe:/:adobe:*acrobat*:4.*" />
            </cpeplcy:platform>
          </cpeplcy:policyDefinition>
        </cdf:check-content>
      </cdf:check>
      - <cdf:check id="AdobeAcrobatPermitted" system="http://permitted.cpe-compliance.dod.mil">
        - <cdf:check-content>
          - <cpeplcy:policyDefinition directive="permitted">
            - <cpeplcy:platform negate="false" operator="OR">
              <cpeplcy:fact-ref name="cpe:/:adobe:*acrobat*:10.*" />
            </cpeplcy:platform>
```

How do I determine my vulnerability risk posture?

- Platform/Patch severity scores will be calculated based on underlying vulnerability scores and distributed to CMRS at Tier 1, 2, and 3 levels
- Severity scores will be uncoupled from policy directives to enable dynamic updates to scores as threat posture changes
- Local administrators can use platform/patch severity scores and CMRS to prioritize remediation activities



Key Takeaways

- All vulnerabilities will be assessed and scored
- Platform and patch-specific compliance policy will replace vulnerability-specific policies
- Vulnerability severity score (0.0 - 10.0) will replace IAVM A/B
- Machine-readable compliance policies (XCCDF/CPE) will be auto-generated and distributed
- Severity scores will be uncoupled from the policy to support dynamic updates based on changes in threat posture

How long is it going to take to get there?

- We're actively working a phased implementation plan
- Asset visibility is our first priority
- Most of the NexGen capabilities will be deployed in FY12/13

IAVM System Points of Contact

- Rob Hyatt: IAVM System Functional Lead (CYBERCOM J34)
  - (443) 479-5722
  - rehyatt@nsa.gov
- Michael Hayes: IAVM System Program Lead (DISA PEO-MA)
  - (717) 267-9295/DSN:570
  - michael.hayes@disa.mil
- Jim Shelton: NexGen IAVM System Program Lead (NSA)
  - (240) 373-2616
  - j.shelto@radium.ncsc.mil
- Greg Decker: IAVM System Contractor Program Manager (Booz Allen Hamilton)
  - (703) 902-4607
  - decker_greg@bah.com