NIST and DISA SCAP Adoption and Integration

NIST National Vulnerability Database
DISA Vulnerability Management System

Presented by:
Peter Mell, NIST
Paul Inverso, DISA

Agenda

- Background
- What is the National Vulnerability Database (NVD)
- How is NVD adopting SCAP?
- What is the DISA Vulnerability Management System (VMS)
- How is VMS adopting SCAP?
- How will NVD and VMS integrate their SCAP capabilities?

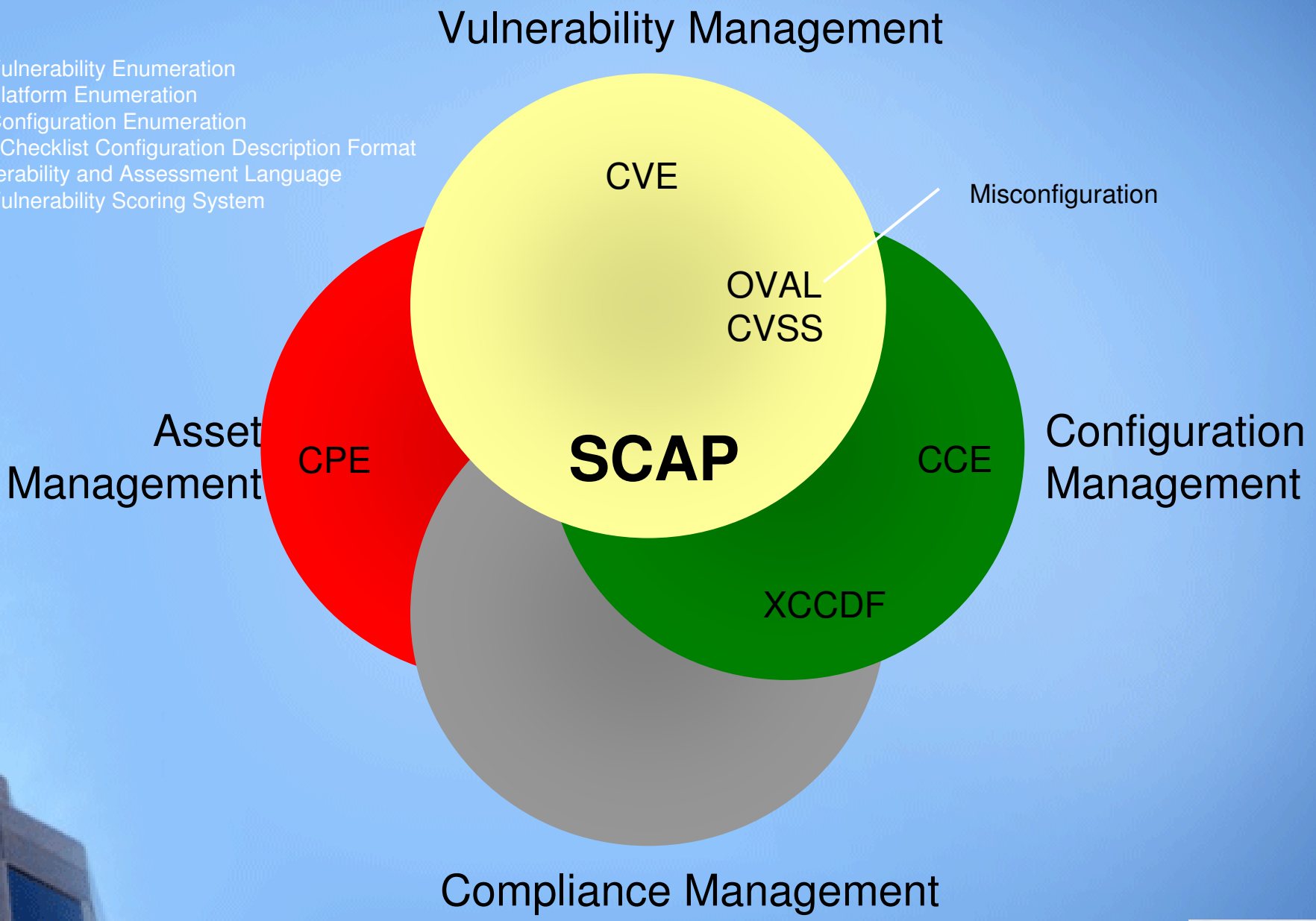
Security Content Automation Protocol (SCAP)

Standardizing How We Communicate

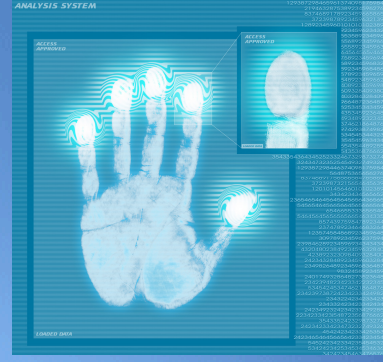
CVE	Common Vulnerability Enumeration	Standard nomenclature and dictionary of security related software flaws
CCE	Common Configuration Enumeration	Standard nomenclature and dictionary of software misconfigurations
CPE	Common Platform Enumeration	Standard nomenclature and dictionary for product naming
XCCDF	eXtensible Checklist Configuration Description Format	Standard XML for specifying checklists and for reporting results of checklist evaluation
OVAL	Open Vulnerability and Assessment Language	Standard XML for test procedures
CVSS	Common Vulnerability Scoring System	Standard for measuring the impact of vulnerabilities

Integrating IT and IT Security Through SCAP

Common Vulnerability Enumeration
Common Platform Enumeration
Common Configuration Enumeration
eXtensible Checklist Configuration Description Format
Open Vulnerability and Assessment Language
Common Vulnerability Scoring System



Computer Network Defense



- Streamline and automate vulnerability and configuration management across the DoD
- Draft DOD CONOPS for SCAP
- SCAP enable the NIST National Vulnerability Database (NVD)
- SCAP enable the DISA Vulnerability Management System (VMS)
- Integrate NVD and VMS

CND is a Defense in Depth approach to enterprise information assurance management

National Vulnerability Database

- NVD is the U.S. government repository of public computer vulnerability information.
- It is designed to be based on and support vulnerability management standards (especially SCAP)
- It receives 69 million hits per year
- Used by Payment Card Industry, Federal Desktop Core Configuration, DHS, GSA Smartbuy, and security products

NVD Program Areas

- Vulnerability Database
  - Security related software flaws
  - 33,000 vulnerabilities
- National Checklist Program
  - Repository of low level checklists for securing OSs and applications
  - 161 checklists
  - Federal Desktop Core Configuration (FDCC) support
- Validation Program
  - Product conformance to the Security Content Automation Protocol (SCAP)
  - 17 validated products, 9 accredited testing laboratories

NVD Current Adoption of SCAP

- Vulnerability Database
  - 32,000 CVEs scored with CVSS and mapped to CPE
  - 16,000 element CPE dictionary
  - 45,000+ product entries in CPE form to be submitted to CPE
  - CVEs are also mapped to the Common Weakness Enumeration (CWE)
- National Checklist Program
  - Migrating checklist content to XCCDF, OVAL, CPE, CCE, and CVE
  - 5 SCAP checklists
  - 17 SCAP beta checklists
- SCAP Validation Program
  - Tests conformance of products against 7 SCAP capabilities
  - Test conformance of products against SCAP component standards individually
    - CVE, CCE, OVAL, and CVSS
  - XCCDF/OVAL Reference Implementation

NVD Future Adoption of SCAP

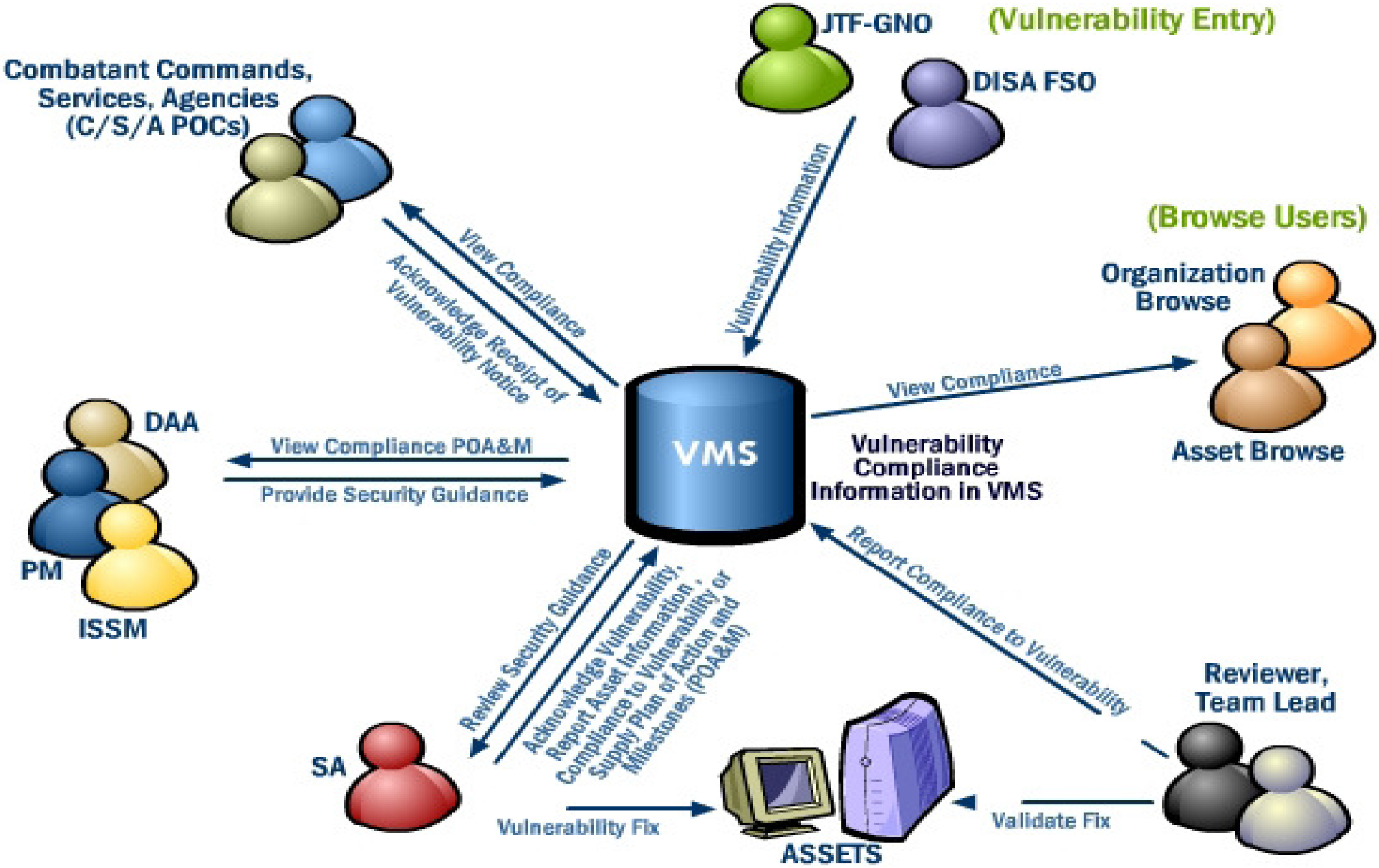
future?

- Analysis and CCSS scoring of CCE
- CPE dictionary maintenance functions
- National Checklist Program XCCDF/OVAL database
- Ability to output custom checklists (set of CPEs, CCEs, and profiles)
- SCAP web services
- SCAP programming API and NVD mirroring capabilities

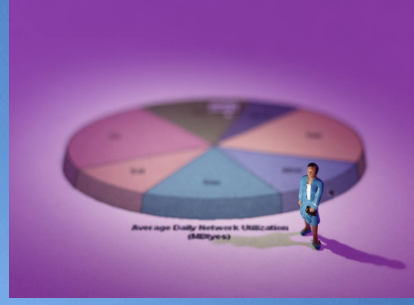
Vulnerability Management System

- VMS assists all DOD CC/S/As in the identification of security vulnerabilities and track the issues through the lifecycle of the vulnerabilities existence.
- Streamlines automation of vulnerability tracking through a relational database and online web views that provide a centralized repository for vulnerability status information and policy compliance information for both NIPRNet and SIPRNet clients.
- VMS information is used for many purposes from practical vulnerability remediation to approval to operate.

VMS Operational View



VMS Capability Areas



- Registration and management of assets (computing and Non-computing), programs, systems, and enclaves
- Vulnerability maintenance
- Vulnerability tracking and record of compliance (Plan of Action and Milestones)
- Audit and inspection results & training
- Notices (vulnerability alerts, tasking orders, warning orders, and other DoD mandated directives)
- And more …

VMS Current SCAP Integration Efforts

- Concept of Operations document collaborate effort with NIST, NSA, and DISA
- Integration Analysis of CPE, CVE, CCE, CCI/SRG, XCCDF, CRF/ARF, OVAL, and CVSS/CCSS
- CPE data mapping to VMS assets
- Defining requirements for future vulnerability maintenance
- Reviewing Asset Model Specification

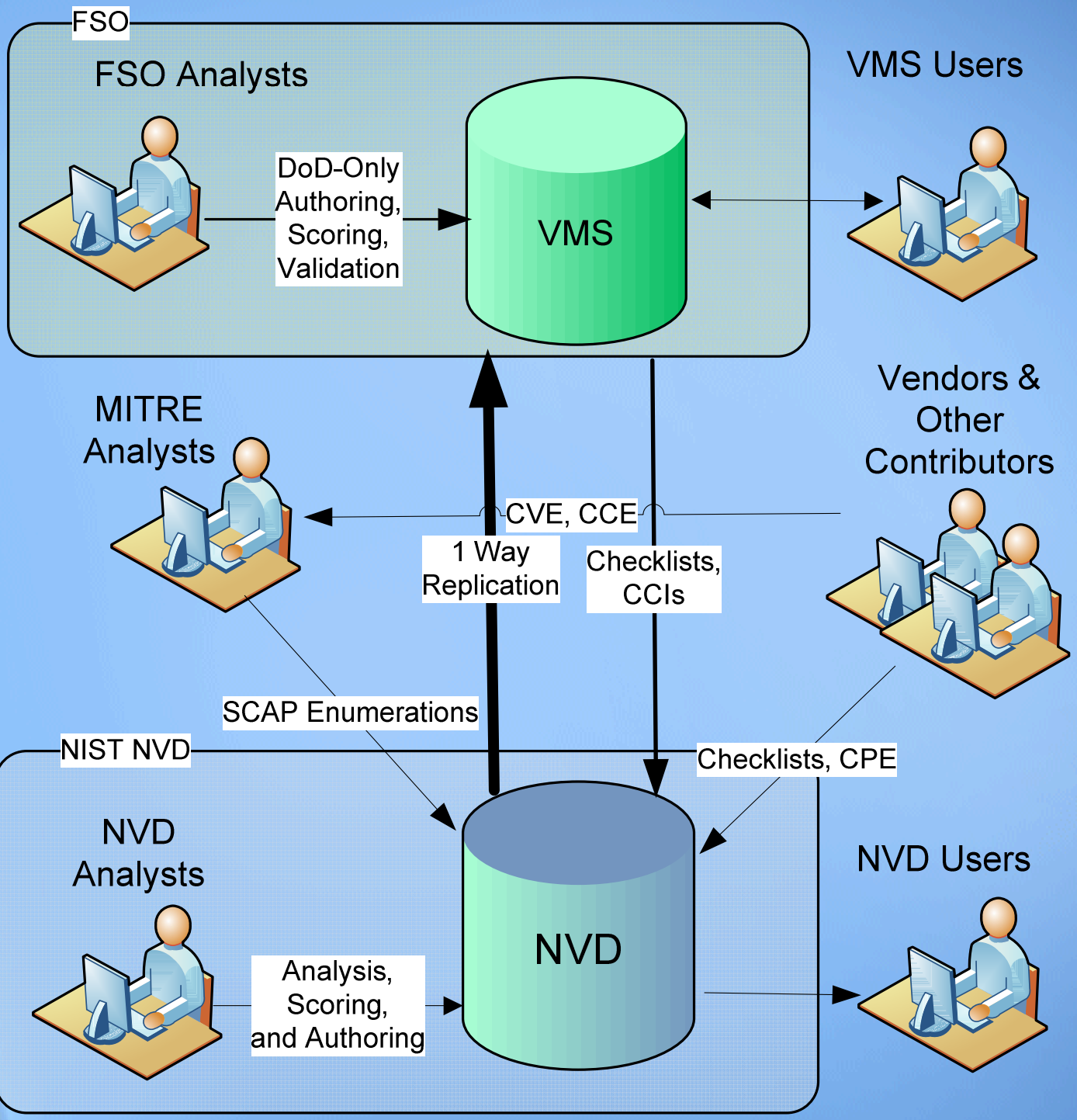
VMS Future Integration into SCAP

future?

VMS Capabilities:

- VMS will ingest/publish vulnerability data from/to NVD
- DISA Field Security Office users will be able to review and validate the content from NVD before being formally accepted into VMS.
- Customizable content
- Store, maintain, generate and update XCCDF and OVAL content.
- Allow the management of non-technical (e.g., policy, or physical security) vulnerability data.
- Interface with other Tier 2 and Tier 3 systems.
- Ingest compliance information from SCAP validated tools.

NVD and VMS SCAP Integration



NVD and VMS SCAP Integration Summary

- MITRE will maintain SCAP enumerations for CVE and CCE
- Public SCAP data will be housed in NVD
- NVD will replicate SCAP data to VMS
- VMS contains DOD-only SCAP data and DOD SCAP compliance data
- VMS will publish DOD SCAP back to NVD as appropriate

Points of Contact

Peter Mell
NIST National Vulnerability Database
301-975-5572
mell@nist.gov

Paul Inverso
DISA Vulnerability Management System
717-267-9921
paul.inverso@disa.mil