Sponsored by
DHS National Cyber Security Division/US-CERT

NIST
National Institute of
Standards and Technolog

National Vulnerability Database

automating vulnerability management, security measurement, and compliance checking

Security Content Automation Protocol (SCAP) Compliance Program

Peter Mell,
National Vulnerability Database
National Institute of Standards and Technology
mell@nist.gov

John Banghart,
Project Lead, SCAP Compliance
John.banghart@nist.gov

July 31 OMB memo to Federal CIOs

"Your agency can now acquire information technology products that are self-asserted by information technology providers as compliant with the Windows XP & VISTA FDCC, and use NIST's Security Content Automation Protocol (S-CAP) to help evaluate providers' self-assertions. Information technology providers must use **S-CAP validated tools**, as they become available, to certify their products do not alter these configurations, and **agencies must use these tools** when monitoring use of these configurations. Related resources (e.g., group policy objects) are also provided to help facilitate agency adoption of the FDCC."

Security Content Automation Protocol (SCAP)

Has Goals...

- Enable standardized and automated vulnerability management, measurement, and policy compliance evaluation (e.g., FISMA and DoD 8500.2/8510 compliance)
- Enumeration of vulnerabilities, misconfigurations, platforms, and impact
- Enable the creation of machine readable security configuration checklists

...Needs Tools

What is an SCAP Compliant Tool?

Tool	CVE	CCE	XCCDF	OVAL	CPE	CVSS
Security Configuration/Vulnerability Scanners	X	X	X	X	X	X
Intrusion Detection Systems	X			X	X	X
Vulnerability Databases	X			X	X	X
Asset Management Tools		X			X	
Policy Framework Tools		X	X		X	
Configuration/Patch Management		X	X	X	X	

The SCAP Compliance Program Should…

- Ensure that security tools
  - comply to the NIST Security Content Automation Protocol (SCAP)
  - be able to certify against one or more the SCAP standards based on the tool function.
- Be unbiased, exact, and process driven
  - How can users trust that they are getting what they need?

National Voluntary Laboratory Accreditation Program (NVLAP)

- Laboratory accreditation programs (LAPs) which are established on the basis of requests and demonstrated need.
- Accredits public and private laboratories based on evaluation of their technical qualifications and competence to carry out specific calibrations or tests.
- Unbiased third-party evaluation and recognition of performance.

SCAP Test Methods and Requirements

- Developed by NIST and shared with the SCAP standards communities
- Provided to NVLAP as input into the overall accreditation program
- Validated on a regular basis
- Updated as needed
  - Significant revisions of SCAP and/or its component standards

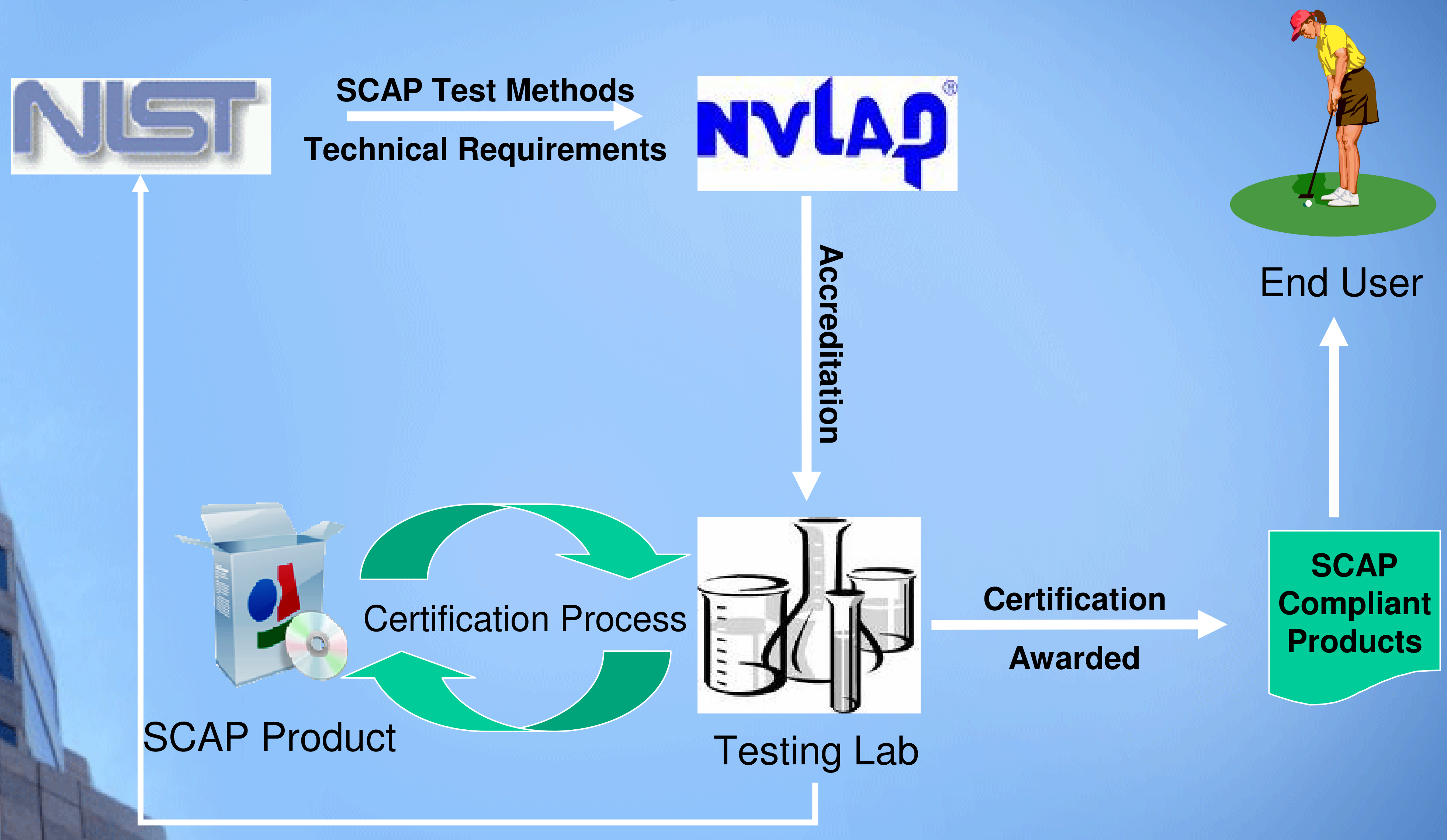
SCAP Configuration Scanning Tool

- Provided by NIST for use in Lab SCAP Compliance testing (e.g. FDCC)
- Purposefully non-competitive with industry tools

The Pieces

- SCAP
- SCAP Test Methods
- NVLAP
- Accredited Testing Labs
- SCAP Products
- End Users

Putting the Pieces Together



SCAP Test Methods

Technical Requirements

Accreditation

End User

Certification Process

SCAP Product

Testing Lab

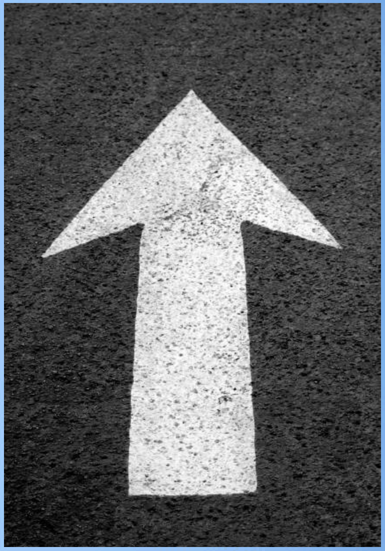
Certification

Awarded

SCAP Compliant Products

Reporting for Validation

Moving Forward



Peter Mell,
National Vulnerability Database
National Institute of Standards and Technology
mell@nist.gov

John Banghart,
Project Lead, SCAP Compliance
John.banghart@nist.gov