



ISAP

Information Security Automation Program

September 2008





ISAP Definition



- **ISAP is a government wide initiative to automate configuration and vulnerability management, security measurement and compliance across agency IT frameworks**
- **SCAP provides the standards that enable security automation**





ISAP Governance



- **Goals**
- **Initiate action to change policy (modify roles and responsibilities) so agency staffing and budgets are established to ensure the long term success of ISAP.**
- **Clarify roles and responsibilities as defined in policy**
- **Ensure effective communication so that required input is received and action taken in a timely way**
- **Connect the security automation strategy to the tactical needs of vendors in implementation**
- **Map responsibilities to standards and identify gaps**





Proposed ISAP Hierarchy

Federal CIO Council

Govern. SC

Technology Infrastructure SubCommittee

Arch. Inf. SC

IP V6 WG

ISAP Working Group (NIST, NSA, DISA, MITRE, ????)

FDCC WG

Recommendations

Recommendations

Directions/Priorities

Coordination

Standards Operation and Development Working Teams (most operated by MITRE)

Formal Change Request

External Advisory Teams (Industry)

Moderation

Technical Requests

Standards Community Working Teams (e.g., discussion lists)

Technical Requests



ISAP Roles & Responsibilities



- **NIST is the public face for vendors and federal agencies, maintains the NVD, publishes checklists, validates products against standards**
- **DISA is the public face for DoD, provides DoD content, issues STIGS and other security guidance**
- **NSA provides resources and leadership in security guidance for the Government and industry**
- **MITRE provides impartial technical advice and leads as moderators on individual technical standards**





ISAP Governance: Working Toward



- A reliable process to capture requirements and change requests
- A process for a predictable revision approval and implementation timeline
- A mechanism for the WG to be better aware of major changes as they are discussed in the user communities
- Ensuring viability of long-term ISAP success
- Having these processes in place by end Nov

