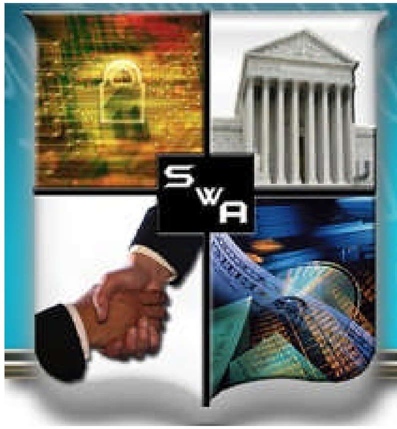


SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

3/4/5 November 2009

DoD-DHS-NIST Software Assurance Forum *The Way Forward for Mitigating Software Supply Chain Risk* Panel Briefing

Facilitator: Marirose Coulson Ziebarth, Booz Allen Hamilton

Homeland Security

Our Panelists

- **Guy Copeland**, VP Information Infrastructure and Advisory Programs and Special Assistant to the CEO, CSC
- **Don Davidson**, Globalization Task Force (GTF) in the Office of the Assistant Secretary of Defense/Network and Information Integration (OASD NII) at US Department of Defense (DoD)
- **Larry Hale**, Director, Office of Infrastructure Optimization, US General Services Administration (GSA)
- **Paul Lewis**, Lead Technologist – Network Security Innovation Platform, Technology Strategy Board, United Kingdom (UK)
- ***Dr. Linda Wilbanks**, CIO, National Nuclear Security Administration (NNSA), US Dept. of Energy (*Mini keynote)
- **Dr. Carol Woody**, Senior Member of the CERT technical staff at the Software Engineering Institute (SEI), Carnegie Mellon University

Session Objectives

- ***Where we are now***: have a dialogue that synthesizes SWA Forum discussions on achieving software assurance in a global marketplace from sessions to date
- ***Where we go from here***: discuss if where we are going is aligned to the Forum's goals and objectives
- ***How we get there***: determine "The Way Forward" by identifying what might be included in an Implementation Road Map and carried forward into the Working Groups

SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

3/4/5 November 2009

DoD-DHS-NIST Software Assurance Forum The Way Forward for Mitigating Software Supply Chain Risk

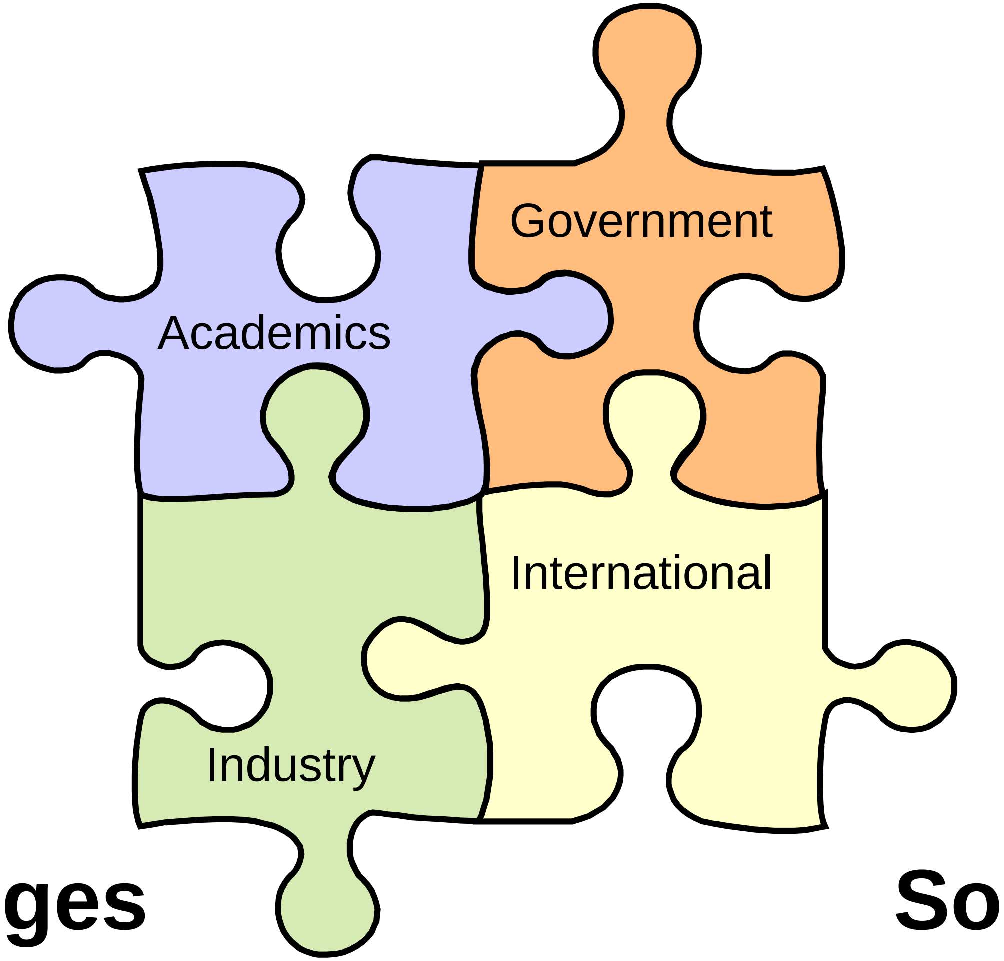
Linda R. Wilbanks, Ph.D.
Chief Information Officer, NNSA

Homeland Security

Defects are built with no malicious intent, then exploited afterwards.

-Joe

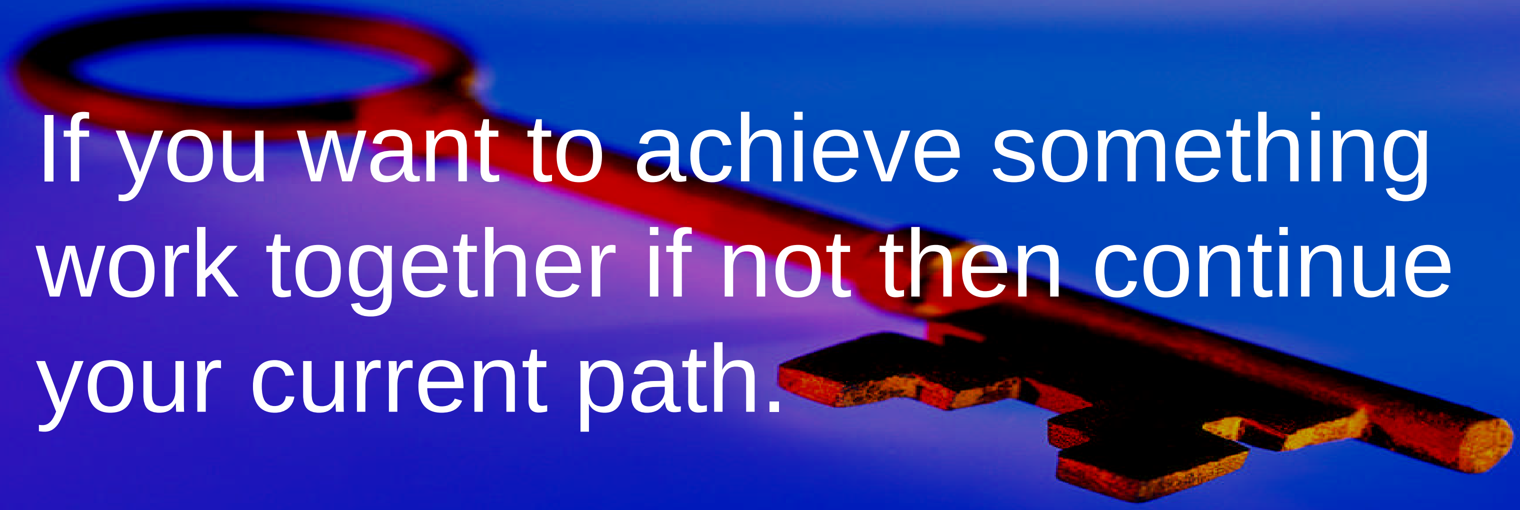
Components



Challenges

Solutions

Enterprise =/= Program



If you want to achieve something work together if not then continue your current path.

“Achieving Software Assurance (SwA) in a Global Marketplace”

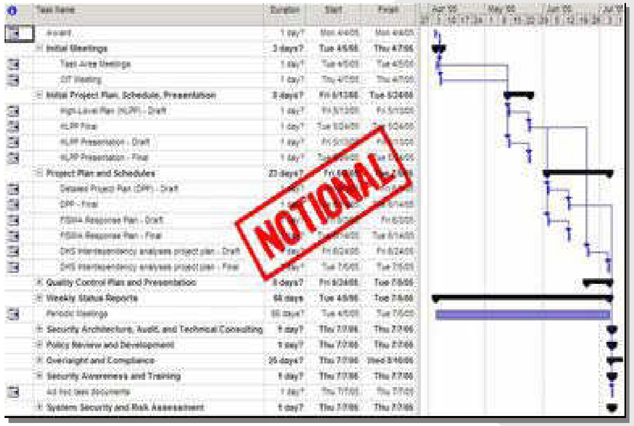
Stakeholders

As Is

- **Government**
- **Industry**
- **Academia**
- **(International)**

“Roadmapping” (POAM)

What is your Organization’s view of the future?
How can SwA Forum help you get there?



Task Name	Duration	Start	Finish
Award	1 day?	Mon 4/4/05	Mon 4/4/05
Initial Meetings	3 days?	Tue 4/5/05	Thu 4/7/05
Task Area Meetings	1 day?	Tue 4/5/05	Tue 4/5/05
OIT Meeting	1 day?	Thu 4/7/05	Thu 4/7/05
Initial Project Plan, Schedule, Presentation	8 days?	Fri 5/13/05	Tue 5/24/05
High-Level Plan (HLPP) - Draft	1 day?	Fri 5/13/05	Fri 5/13/05
HLPP Final	1 day?	Tue 5/24/05	[illegible]
HLPP Presentation - Draft	1 day?	[illegible]	[illegible]
HLPP Presentation - Final	1 day?	[illegible]	[illegible]
Project Plan and Schedules	23 days?	[illegible]	[illegible]
Detailed Project Plan (DPP) - Draft	[illegible]	[illegible]	[illegible]
DPP - Final	[illegible]	[illegible]	[illegible]
FISMA Response Plan - Draft	[illegible]	[illegible]	Fri 6/3/05
FISMA Response Plan - Final	[illegible]	[illegible]	Tue 6/14/05
DHS interdependency analyses project plan - Draft	[illegible]	Fri 6/24/05	Fri 6/24/05
DHS interdependency analyses project plan - Final	[illegible]	Tue 7/5/05	Tue 7/5/05
Quality Control Plan and Presentation	8 days?	Fri 6/24/05	Tue 7/5/05
Weekly Status Reports	66 days	Tue 4/5/05	Tue 7/5/05
Periodic Meetings	66 days?	Tue 4/5/05	Tue 7/5/05
Security Architecture, Audit, and Technical Consulting	1 day?	Thu 7/7/05	Thu 7/7/05
Policy Review and Development	1 day?	Thu 7/7/05	Thu 7/7/05
Oversight and Compliance	25 days?	Thu 7/7/05	Wed 8/10/05
Security Awareness and Training	1 day?	Thu 7/7/05	Thu 7/7/05
All Hot Item Documents	1 day?	Thu 7/7/05	Thu 7/7/05
System Security and Risk Assessment	1 day?	Thu 7/7/05	Thu 7/7/05

Working Groups

Measures

- **People**
- **Process**
- **Technology**
- **Acquisition**

What does your WG’s “pathway” look like?
Who participates to develop what?

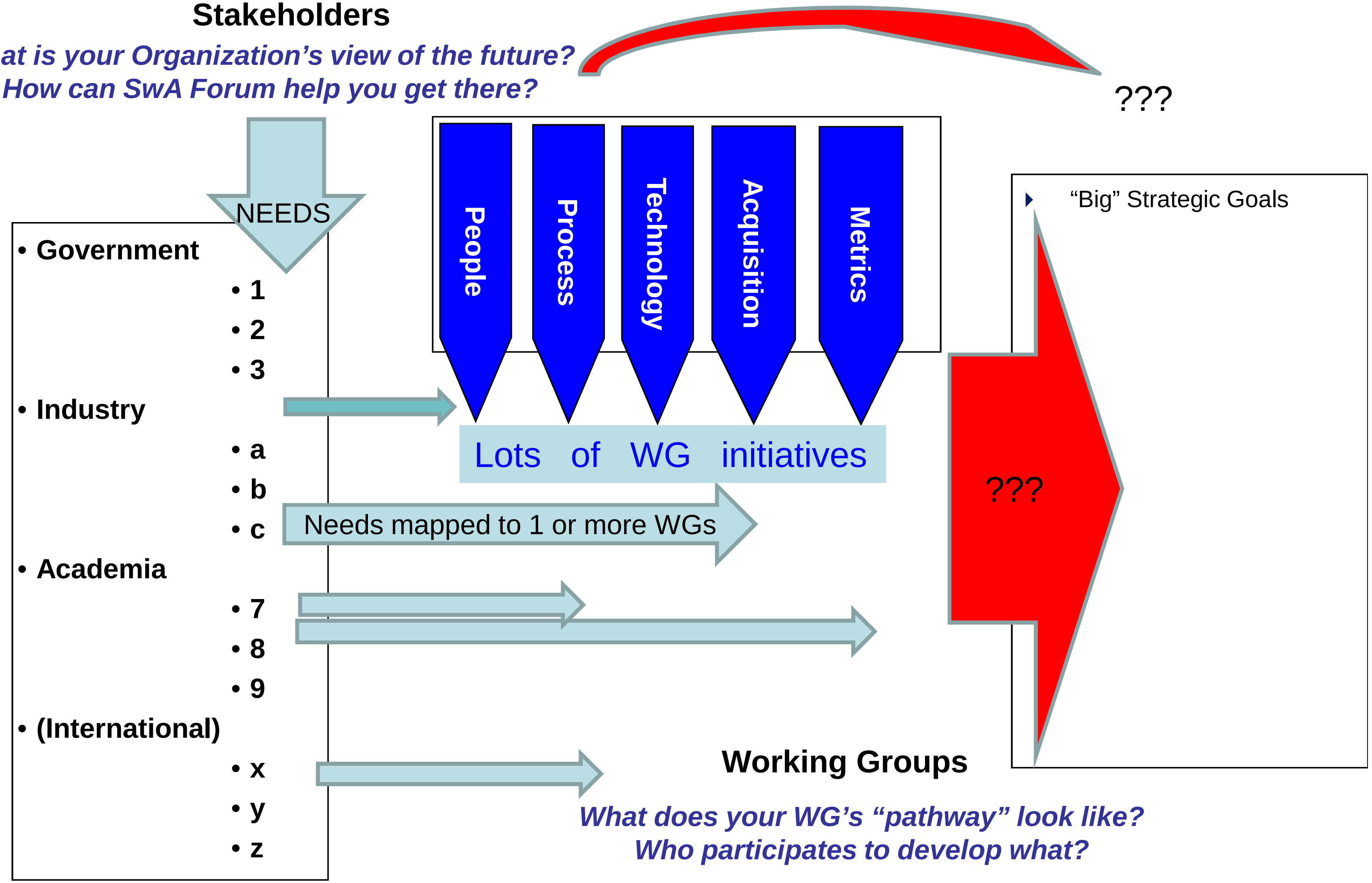
To Be ?

- Trustworthy systems
- w/ Managed Risk from SW we develop, acquire, use / “rely on”…
- Enabled by
  - “Built in Security”
  - Informed acquisition
  - Transparent supply chains
  - Real Life Cycle Mgt

Our goal is to develop a high level Implementation Road Map for use of our WGs during their Dec’09 Work Sessions.

Stakeholders

What is your Organization's view of the future?
How can SwA Forum help you get there?



NEEDS

- **Government**
  - **1**
  - **2**
  - **3**
- **Industry**
  - **a**
  - **b**
  - **c**
- **Academia**
  - **7**
  - **8**
  - **9**
- **(International)**
  - **x**
  - **y**
  - **z**

People | **Process** | **Technology** | **Acquisition** | **Metrics**

Lots of WG initiatives

Needs mapped to 1 or more WGs

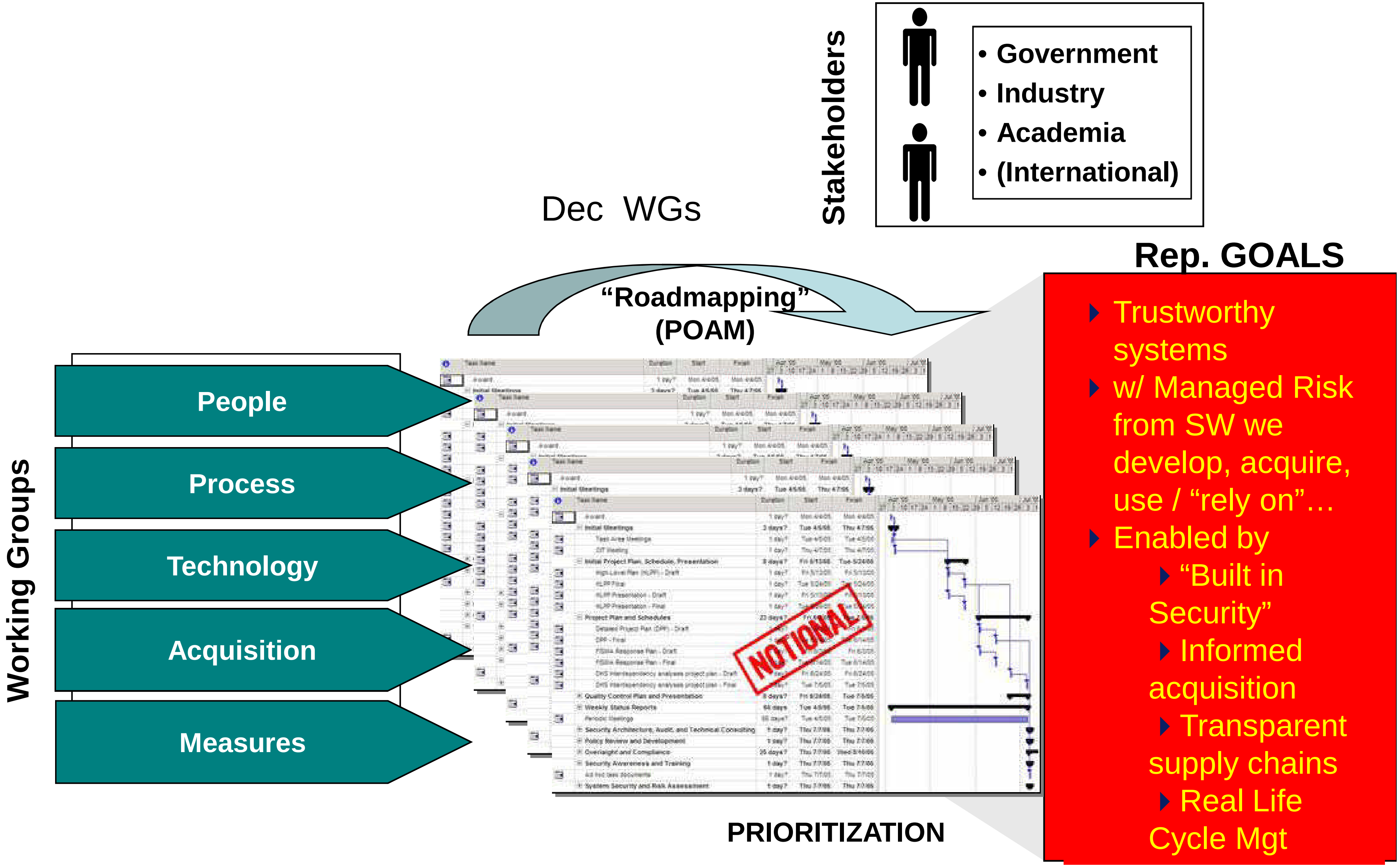
???

???

- "Big" Strategic Goals

Working Groups

What does your WG's "pathway" look like?
Who participates to develop what?



Stakeholders

- Government
- Industry
- Academia
- (International)

Dec WGs

“Roadmapping” (POAM)

Working Groups

PRIORITIZATION

Rep. GOALS

- Trustworthy systems
- w/ Managed Risk from SW we develop, acquire, use / “rely on”…
- Enabled by
  - “Built in Security”
  - Informed acquisition
  - Transparent supply chains
  - Real Life Cycle Mgt

Our goal is to develop a high level Implementation Road Map for use of our WGs during their Dec’09 Work Sessions.

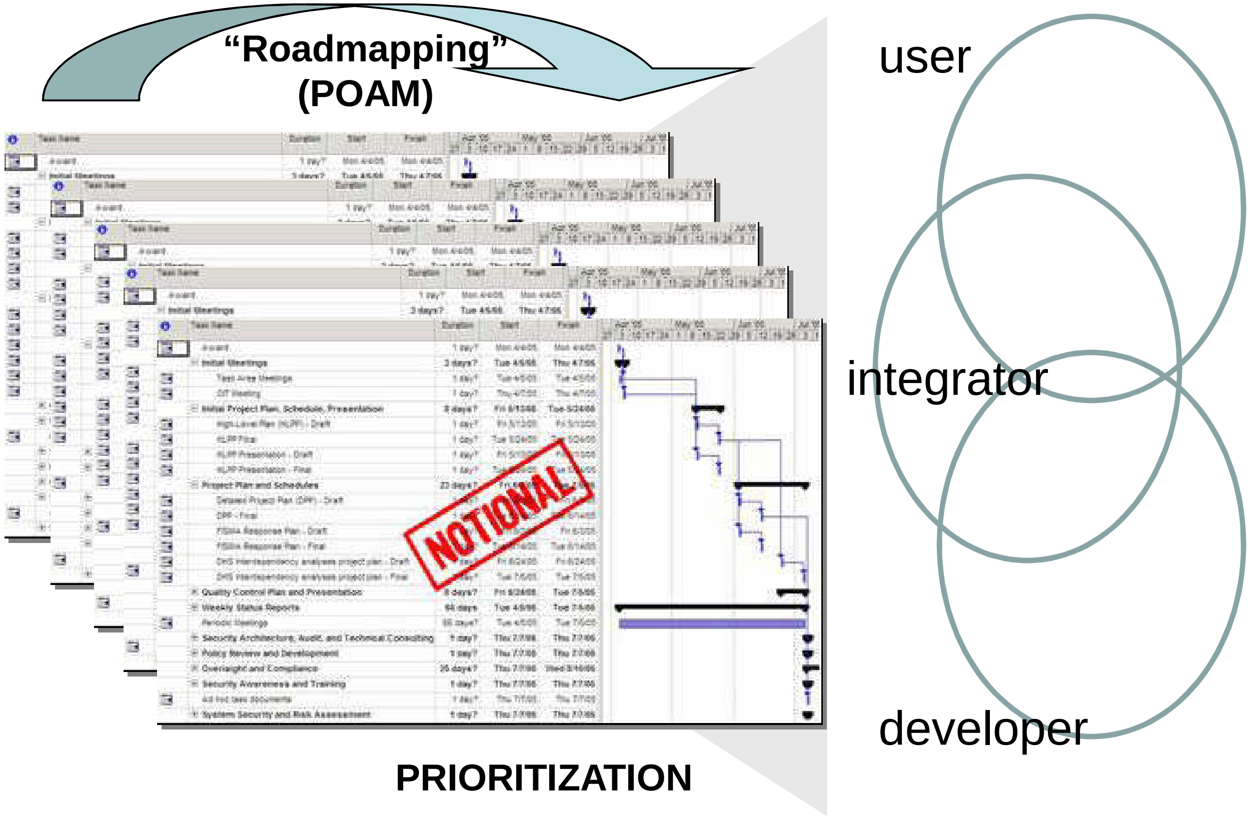
Rep. GOALS

- Trustworthy systems
- w/ Managed Risk from SW we develop, acquire, use / “rely on”…
- Enabled by
  - “Built in Security”
  - Informed acquisition
  - Transparent supply chains
  - Real Life Cycle Mgt

Dec WGs

Stakeholders

- Government
- Industry
- Academia
- (International)



Task Name	Duration	Start	Finish
Award	1 day?	Mon 4/4/05	Mon 4/4/05
Initial Meetings	3 days?	Tue 4/5/05	Thu 4/7/05
Task Area Meetings	1 day?	Tue 4/5/05	Tue 4/5/05
OIT Meeting	1 day?	Thu 4/7/05	Thu 4/7/05
Initial Project Plan, Schedule, Presentation	8 days?	Fri 5/13/05	Tue 5/24/05
High-Level Plan (HLPP) - Draft	1 day?	Fri 5/13/05	Fri 5/13/05
HLPP Final	1 day?	Tue 5/24/05	Tue 5/24/05
HLPP Presentation - Draft	1 day?	[illegible]	[illegible]
HLPP Presentation - Final	1 day?	[illegible]	[illegible]
Project Plan and Schedules	23 days?	[illegible]	[illegible]
Detailed Project Plan (DPP) - Draft	[illegible]	[illegible]	[illegible]
DPP - Final	[illegible]	[illegible]	[illegible]
FISMA Response Plan - Draft	[illegible]	[illegible]	Fri 6/3/05
FISMA Response Plan - Final	[illegible]	[illegible]	Tue 6/14/05
DHS Interdependency analysis project plan - Draft	[illegible]	Fri 6/24/05	Fri 6/24/05
DHS Interdependency analysis project plan - Final	1 day?	Tue 7/5/05	Tue 7/5/05
Quality Control Plan and Presentation	8 days?	Fri 6/24/05	Tue 7/5/05
Weekly Status Reports	66 days	Tue 4/5/05	Tue 7/5/05
Periodic Meetings	66 days?	Tue 4/5/05	Tue 7/5/05
Security Architecture, Audit, and Technical Consulting	1 day?	Thu 7/7/05	Thu 7/7/05
Policy Review and Development	1 day?	Thu 7/7/05	Thu 7/7/05
Oversight and Compliance	26 days?	Thu 7/7/05	Wed 8/10/05
Security Awareness and Training	1 day?	Thu 7/7/05	Thu 7/7/05
Ad hoc task documents	1 day?	Thu 7/7/05	Thu 7/7/05
System Security and Risk Assessment	1 day?	Thu 7/7/05	Thu 7/7/05

Apr '05 May '05 Jun '05 Jul '05

PRIORITIZATION

Our goal is to develop a high level Implementation Road Map

Which delivers products to be used (where / how?)…

DoD-DHS-NIST Software Assurance Forum Panel: The Way Forward 5 November 2009

CSC

Guy Copeland, Vice President
Information Infrastructure Advisory Programs and
Special Assistant to the CEO, CSC

Homeland Security

Trends, Issues, Thoughts, Suggestions

- Some growing emphasis on compliance as competitive edge
- Need for continuous supply chain risk assessment analysis
- Rapid, flexible, trusted supply chain formation for NS/EP
- Capitalize on commonality of need for commercial and government
- Risk management means risk management, not risk free
- Risk should be shared fairly
- Develop standards, practices, protocols and other agreed controls through true public-private partnership
- Role of identity management (HW, SW, people)
- Solutions must work internationally