

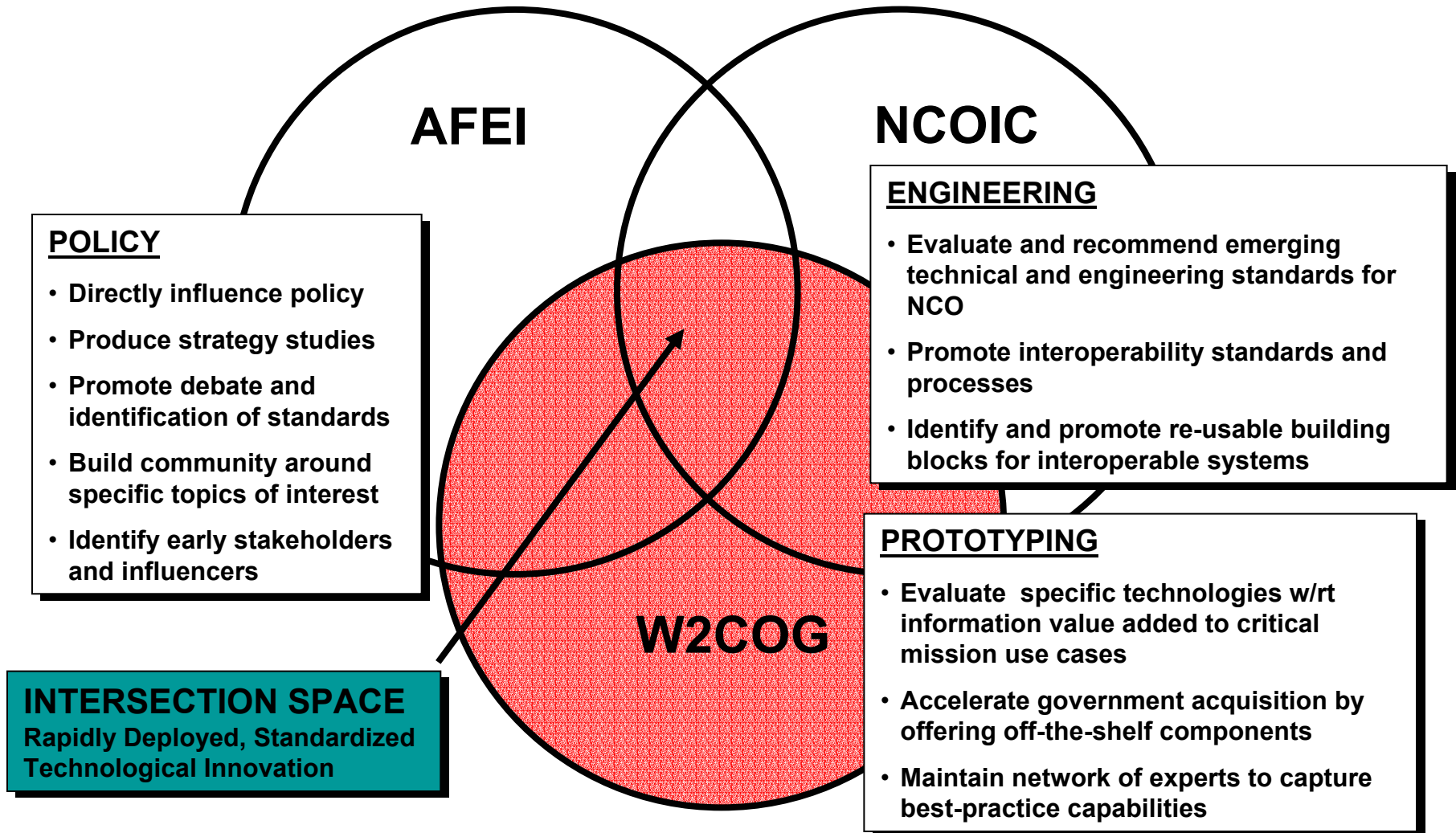
Industry Support for DoD: A Collaborative Model that Works

Greg Gardner

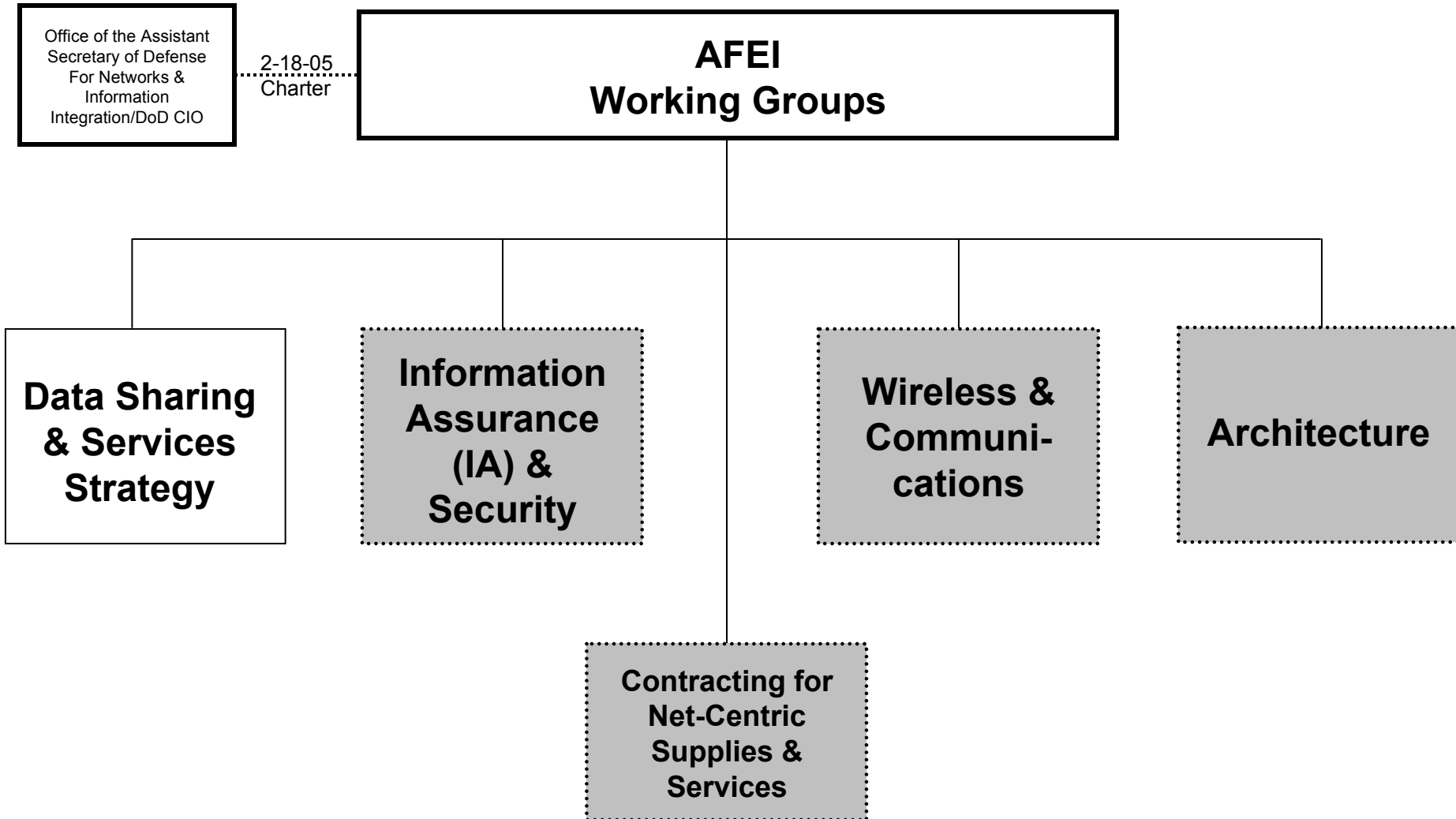
VP, Government and Homeland Security
Solutions

Oracle Corporation

Who's who...?



Association for Enterprise Integration



Data Sharing WG Contributors:

- Absolute Computer Tech
- BAE SYSTEMS
- Booz Allen Hamilton
- Battelle Memorial Institute
- Boeing
- CACI
- CISCO
- Data Systems Analysts, Inc.
- DNC
- Eagan McAllister Associates
- EDS
- EMSolutions
- Forrester Research
- IBM
- Institute for Defense Analysis
- Intelligent Decisions Inc
- Graves Corner Group
- Green Hills Software
- Lockheed Martin
- McDonald Bradley
- Metamatrix
- Microsoft
- Mitre
- Northrop Grumman
- Oracle
- Raytheon
- Reactivity
- Rockwell-Collins
- Sun Microsystems
- SIGABA
- SRA
- Systinet
- Titan
- Unisys
- Weblayers
- Westbridge Technology

Special Thanks...

- Joan Baumstarck (EDS) (Co-Chair)
- Ed Barger, (Boeing)
- Michael Crooks (WebLayers, Inc.)
- Marty Dowd (L-3 Communications Titan)
- Moses Kamai (Battelle Memorial Institute)
- Charlie Kille (Raytheon Company)
- Laura Lee (SPARTA, Inc.)
- JoLee Loveland Link (Volvox, Inc.)
- John Link (Volvox, Inc.)
- Hans Polzer (Lockheed Martin)
- Arnie Rausch (Eagan McAllister Assoc, Inc.)
- Andras Szakal (IBM)

AFEI WG Charter

(signed by DoD CIO 18 Feb 2005)

1. Support the migration to an open business model that supports full competition but enables horizontal integration of the resulting capabilities and systems, regardless of who developed or provides the system.
2. Review and comment on industry-wide frameworks which will support horizontal integration of platforms and systems.
3. Provide an industry advisory service for the DoD CIO regarding net-centric strategies, programs, acquisitions, implementation, and containment.
4. Provide industry-wide critiques and analysis in response to government stakeholders.
5. Provide a forum for industry discussion and collaboration on evolving enterprise service models.
6. Annually review the continuing benefits of this committee and take appropriate action to dissolve or continue

Data Sharing WG Accomplishments

- White Paper, “Responding to the Challenges of Net Centric Operations,” Nov 17, 2004
- White Paper, “Industry Best Practices for Achieving Service Oriented Architecture,” Apr 22, 2005
- White Paper, “Facilitating Shared Services in the DoD,” Feb 12, 2006
- White Paper, “Shared Services: Performance Accountability and Risk,” initial draft in development...due early Summer 2006

Responding to the Challenges of Net Centric Operations: The Questions Asked

- How can OSD NII be more effective in “getting the word out” to all net-centric stakeholders?
- How best to approach industry standards?
- What does industry need from government to address new business models?

Responding to the Challenges of Net Centric Operations: Report Summary

- Increase the AFEI Support Role
 - Regular outreach and education
 - Standing working groups and tasking
 - Access to Government
- Task AFEI to create candidate Standards Governance Infrastructure framework and present to DoD CIO
- Request AFEI draw together net-centric organizations for more efficient and effective dialog with DoD
 - NCOIC, W2COG, W3C, OMG, OASIS, IEEE, Etc⁹

Industry Best Practices for Achieving SOA: Task

- Recommend acquisition models that DoD could use to acquire services and for industry to provide services.
- Explore the role of information technology (IT) integrators and vendors in a Service Oriented Architecture (SOA) environment.
- Provide industry input on best commercial practices, service environment business models, internal industry practices, and applicability of those practices and models to DoD.
- Address interest, risk, liabilities, advantages & disadvantages of industry opn of Global Information Grid Enterprise Services (GIG ES).
- ...and...review lessons learned from managed service efforts and industry business cases.

Industry Best Practices for Achieving SOA: Report Summary

- Report only “frames the starting point” for SOA analysis
- First iteration of SOA discussions:
 - Rapidly evolving technology and best practices
 - Contains basic explanations of SOA and services
 - Non-technical
 - Consensus views
- “...the principal lesson of this study is that SOA is simply a tool that must be implemented by engaged, attentive, and committed senior leaders who demand a culture of information sharing and improved organizational effectiveness.”

Facilitating Shared Services: Task

“What should be the tenets of DoD policy that constrain industry and the government from developing redundant services, that incentivize industry and the government to reuse services, as they become available, and that mitigate the risks to both industry and the government of employing those services across distinct programs.”

Facilitating Shared Services: Focus Areas

- Governance and Control Policy
- Common Information Standards and Technical Standards Policy
- Security, Trusted Information and Certification Policy
- Performance Accountability and Risk Policy
- Incentives for Government and Industry

Governance and Control Policy

- Definition:
 - *Provides the legal and management processes to ensure services sharing*
- Top 3 Issues:
 - Lack of awareness of existing services, no mechanism to discover existing services
 - No process for getting mods on reused services funded and prioritized
 - Risk of independent, non-collaborative portfolios
- Top 3 Recommendations:
 - Portfolio managers as ‘guardians’ w/ process to collect and exchange information on emerging needs and on planned services
 - DoD CIO implement DODD 8115.01 to lead a cross-Mission Area governance forum (i.e. an Enterprise Portfolio Managers’ board) to oversee Enterprise Portfolio Monitoring of DoD Portfolios
 - Recommend that Military Service-based acquisition practices be flagged as an issue for resolution by DoD

Common Information Standards and Technical Standards Policy

- Definition:
- *Provides the policy to enable interoperability in shared-services by creating common standards for the multiple net-centric communities & technologies.*
- Top 3 Issues:
 - There is a critical need for common standards that address SOA core services with enough detail to eliminate vendor differences
 - Industry is not motivated to provide a seamless, heterogeneous SOA infrastructure
 - Standards for SOAs and net-centric operations are currently unclear, evolving, and potentially competitive
- Top 3 Recommendations:
 - The differentiation between standards and requirements needs to be clearly defined
 - To ensure a “need to share” framework, DoD CIO must define the common information and technical standards for shared-services and codify these into a “Book of Knowledge” to be used by those who do business with DoD
 - SOA standards need to be extended to eliminate vendor specific solutions that prevent interoperability

Security, Trusted Information and Certification Policy

- Definition:

- *Describes policy needed to support the parallel challenges of assuring information access and interoperability, while maintaining necessary security and trust in both information and information-sharers.*

- Top 3 Issues:

- Due to prolonged security processes, C&A of new services and technologies is often obtained long after they are mature and ready for use
- A core obstacle to information sharing is the security process
- Lack of awareness of existing services, no mechanism to discover existing services
- Secure and trusted information involves a complex (and sometimes contradictory) set of issues revolving around “trust”

- Top 3 Recommendations:

- Each portfolio and sub-portfolio should have a single Designated Approving Authority (DAA) Officer
- DoD CIO needs to fast-track the establishment of a cross-community C&A mechanism
- Establish a security framework that supports authentication and authorization based on a common set of user attributes

Performance Accountability and Risk Policy

- Definition:
 - *Describes policies to mitigate risk to both industry and government employing reusable services across distinct programs.*
- Top 3 Issues:
 - Inadequate confidence in existing services availability, reliability and Key Performance Parameters
 - Little government guidance on approved, certified or available services that should be reused by industry and other government programs
 - No mechanism to learn about an existing service's performance record
- Top 3 Recommendations:
 - Historical performance records on available services need to be made more visible
 - Interoperability testing policy, as currently provided in DODD 4630.5 / DODI 4630.8, is focused on technical standards. Policy should be modified to address cross-domain *mission* interoperability within and between portfolios as the SOA environment grows
 - Additional government guidance for program managers (PMs) should be developed to address the issue of life cycle service liability of service providers for shared-services

Incentives for Government & Industry

- Definition:
 - *Describes policy that provides a favorable climate, inducement, and/or reward for sharing services; or provides a deterrent or penalty for not sharing services.*
- Top 3 Issues:
 - PMs (consumers) and industry (service providers) are neither required nor motivated (beyond basic budget savings) to reuse existing services
 - There is no mechanism in place to address the liability for the contractor or PM who proposes to reuse existing services from outside of their program
 - Existing services rarely satisfy new users without discussion and collaboration. There is no incentive system that fosters government agencies and industry to seek this discussion and collaboration.
- Top 3 Recommendations:
 - DoD should adopt monetary, non-monetary and hybrid incentive models that foster service sharing
 - A core service (e.g., Enterprise Service Management) should be required to collect the necessary usage information to support “fee-for-service” or “pay-by-the-click” models, aligning service provider actions with service consumer needs
 - The Defense Acquisition System needs to incorporate evaluation criteria for service reuse, akin to the “small business credit”, that places greater weight on reuse of available services in new capability proposals.

DoD CIO Follow up...

- Request for 10 focused papers...
- First 3:
 - Late Spring 2006
 - Tenet: Common Information Standards and Technical Standards
 - The goal of the DoD is to promote an SOA development that is also net-centric. Describe the characteristics of an architecture that is both net-centric and service-oriented, and map that to existing/new DoD Architectural Framework (DoDAF) products.
 - Late Spring 2006
 - Tenet: Government and Industry Incentives
 - What specific changes, if any, would industry recommend for the DODD 5000 acquisition process to maximize the value of services for the Department? For example, what changes would industry recommend for Milestone A, B, and/or C deliverables for a predominantly service based program or a program that is planning on using multiple services in delivering capabilities?
 - **Early Summer 2006**
 - **Tenet: Performance Accountability and Risk**
 - **If industry were going to reuse a service in the development of a capability, what performance metrics would government need to publish in order for industry to have adequate confidence in the consumed service?**

DS3 Team Next Steps

- Refine definition of “Net-centric” in Task 1 by 31 March and hand off to AFEI
- Define requirements for C&A by 31 March and hand off to AFEI
- Initial draft of response to Task 3 by 31 March...then begin iterative refinement

Conclusions

- Model works; mutual value
- Evolutionary process
- Hard work required
- Lots to do
- Join us...