Service Oriented Architecture (SOA) for DoD

Prof. Paul A. Strassmann

January 9, 2008
Part 1

SOA Requirements
The DoD Challenge

DoD use of SOA
Most DoD Projects Have Own Data

<table>
<thead>
<tr>
<th>Projects</th>
<th>07 Budget $ Millions</th>
<th>Number of Projects</th>
<th>% of Total Budget $</th>
<th>% of Projects</th>
</tr>
</thead>
<tbody>
<tr>
<td>Project - &gt; $100 Million</td>
<td>$10,301</td>
<td>43</td>
<td>33.9%</td>
<td>1.3%</td>
</tr>
<tr>
<td>Projects - &gt; $10 Million</td>
<td>$15,013</td>
<td>525</td>
<td>49.4%</td>
<td>15.4%</td>
</tr>
<tr>
<td>Projects - &lt; $10 Million</td>
<td>$5,066</td>
<td>2,832</td>
<td>16.7%</td>
<td>83.3%</td>
</tr>
<tr>
<td>Total</td>
<td>$30,380</td>
<td>3,400</td>
<td>100.0%</td>
<td>100.0%</td>
</tr>
</tbody>
</table>

DoD use of SOA
What is a Network Centric SOA?

The capacity to:

Discover Applications Anywhere;
Display the Capabilities of All Applications;
Discover Network Data from a Data Registry;
Mediate the Extraction of Information From Data Bases;
Execute Unique Requests through Using Multiple Servers;
Provide Credentials Validation and Security to Everyone;

Generate Responses at “Google Speed” ( <1 second).
SOA for Interoperability

**DoD use of SOA**
Existing Systems Cannot Respond in Google-Time
Policies For SOA Exist (Partial List)

- DoDI 8110.1 “Multinational Information Sharing Networks Implementation”.

- DoD Net-Centric Data Management Strategy: Metadata Registration, April 3, 2003
- DoD Net Centric Strategy, May 9, 2003
- Department of Defense Discovery Metadata Specifications
- DEPSECDEF Memorandum on “Information Technology Portfolio Management”, March 22, 2004
- Director of Central Intelligence, “Intelligence Information Sharing”, June 9, 2004

DoD use of SOA
ASD NII / DoD CIO Is in Charge

DoD Directive 5144.1, May 2, 2005:

- Initiates continuation, modification or termination of programs;
- Concurs with budget requests;
- Ensures enforcement of policies and standards;
- Assures compliance with standards & policies;
- Dictates data & information management methods;
- Has direct authority over the Director of DISA;
- Issues DoD Instructions.

DoD use of SOA
Foundation of DoD SOA

DoD Directive 8320.02, Data Sharing

- Data shall be visible, accessible, and understandable to any user.
- Data assets shall be made visible by associating metadata ("tagging") for each data asset.
- Data assets shall be made understandable by publishing semantic and structural metadata in a DoD metadata registry.
A Requirement for DoD SOA

DoD Directive 8320.03, Unique Identification

- All business, warfighter, intelligence, and enterprise information environment transactions, among the Department of Defense, Federal and State Agencies, non-governmental organizations, and domestic and foreign persons and organizations will use Unique Identification (UID) standards.
DoD Infrastructure Costs are Excessive ($ Millions*, I.T. Costs)

<table>
<thead>
<tr>
<th>Function</th>
<th>Total 07 Spending</th>
<th>% of Total Spending</th>
</tr>
</thead>
<tbody>
<tr>
<td>Warfighter Missions</td>
<td>$10,876</td>
<td>36%</td>
</tr>
<tr>
<td>IT Infrastructure</td>
<td>$14,185</td>
<td>47%</td>
</tr>
<tr>
<td>Logistics</td>
<td>$2,377</td>
<td>8%</td>
</tr>
<tr>
<td>HR Management</td>
<td>$1,834</td>
<td>6%</td>
</tr>
<tr>
<td>Finance &amp; Administration</td>
<td>$1,036</td>
<td>3%</td>
</tr>
<tr>
<td>Other</td>
<td>$185</td>
<td>1%</td>
</tr>
<tr>
<td><strong>Total DoD FY 07</strong></td>
<td><strong>$30,492</strong></td>
<td><strong>100%</strong></td>
</tr>
</tbody>
</table>
### Problem: DoD Contractors Build Separate Infrastructures

<table>
<thead>
<tr>
<th></th>
<th>FY05</th>
<th>FY06</th>
<th>FY07</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Total DoD I.T. Spending</strong></td>
<td>$28.7</td>
<td>$29.9</td>
<td>$30.4</td>
</tr>
<tr>
<td><strong>DoD Spending on Contractors</strong></td>
<td>$21.1</td>
<td>$22.6</td>
<td>$24.1</td>
</tr>
<tr>
<td><strong>% of I.T. Spending Contracted Out</strong></td>
<td>73.5%</td>
<td>75.6%</td>
<td>79.3%</td>
</tr>
</tbody>
</table>
Part 2

SOA Concepts
DoD Pursues “Federation” or “Tiered Accountability” for SOA

POLICY:
• Units in DoD shall operate under a common set of rules.
• SOA is based on trust and security among autonomous units.

PROBLEMS:
• Where and when do common SOA rules apply?
• How will SOA trust and security be established?
Problem: Who Oversees SOA?

(Partial List)

- DoD CIO Executive Board (CIO EB)
- Military Communications and Electronics Board (MCEB)
- GIG E2E Systems Engineering Advisory Board (SSEB)
- IT Standards Oversight Panel (ISOP)
- Information Assurance Senior Leadership Group (IASLG)
- Interoperability Senior Review Panel (ISRP)
- GIG Waiver Board and Panel
- DISN Flag Panel
- DISN Designated Approving Authority (DAA)
- DISN Security Accreditation Working Group (DSAWG)
- DIAP (Defense-Wide Information Assurance Program.)
- Joint Battle Management Board (JBM C2 BoD)
- Defense Business Systems Management Committee (DBSMC)
- CCB (Configuration Control Board)
Who Builds SOA?

- The United States Strategic Command (USSTRATCOM) is responsible for planning, integrating, and coordinating DoD’s NetOps.
- The DoD GIG is executed by Joint Task Force Global Network Operations (JTF/GNO) through DISA.
- Business Transformation Agency develops systems.

- SOA components to be shared:
  - **Service Discovery** - *(Services Discoverable in Directory)*
  - **Enterprise Service Management** - *(Display of Services Capabilities)*
  - **Mediation** - *(Enables Extraction of Information)*
  - **MetaData Registry** - *(Enables Discovery of Data)*
  - **Messaging** - *(Ability to Different Servers to Execute a Task)*
  - **People Discovery** - *(Single Source for Identification)*
  - **Service Security** - *(Credentials validation, Security processes)*
  - **Application Hosting**
According to H.R. 1585 the DoD Chief Management Officer, with support from Service Undersecretaries for Management:

1. Will also act as the Management Officers of the Army, Navy and the Air Force.
2. Will approve budgets for changes to policies, procedures, processes, and systems.
3. Will approve budget requests for business systems submitted to Congress.
Concept How to Organize SOA

Programs

Army, Navy, Air Force

Agencies

Combatant Commands

Business Mission

WarFighting Mission

Intelligence Mission

Enterprise Information Environment

Focus of this Presentation

DoD use of SOA
## SOA Concept

### Business Mission Area (BMA)
- **DoD Lead:** BTA

#### Governance
- Acquisition
- Financial Management
- Human Resource Management
- Logistics
- Installations & Environment
- Civil Works

### Warfighting Mission Area (WMA)
- **DoD Lead:** CJCS

#### Governance
- Battlespace Awareness
- Force Application
- Protection
- Focused Logistics
- Battlespace Communications

### Information Assurance
- **Domain Owner:** Director, Information Assurance

#### Core Enterprise Services
- Communications
- Computing Infrastructure
- Core Enterprise Services

### Enterprise Information Environment Mission Area (EIEMA)
- **DoD Lead:** DoD CIO/ASD(NII)

---

**DoD use of SOA**
Organization of Infrastructure Services for SOA

Infrastructure Services
(Enterprise Information)

- Data Services
- Security Services
- Computing Services
- Communication Services
- Application Services
Organization of Data Services

Data Services

- Discovery Services
- Management Services
- Collaboration Services
- Interoperability Services
- Semantic Services
Fundamental Data Principles

- Data, services and applications belong to the Enterprise.
- Data are a strategic asset.
- Data and applications cannot be coupled to each other.
- Data must be visible outside of the applications.
- Data should be obtained from dictionary, not summaries.
- Semantics and syntax is defined by a community of interest.
- Data must be trusted by casual user.

ISSUE
- How will individual projects comply?
- How will data be extracted from legacy databases?
Organization of Communication Services

Communication Services

- Interoperability Services
- Spectrum Management
- Connectivity Arrangements
- Continuity of Services
- Resource Management

DoD use of SOA
• GIG shall enable users to access and share information from any location, at any time.
• GIG shall be implemented as a unified enterprise under a central authority.

ISSUE
• How will individual projects integrate?
• How will GIG offer end-to-end connectivity?
• How will low latency be assured throughout?
• How will existing networks become integrated into GIG?
Organization of Computing Services

Computing Services

- Computing Facilities
- Resource Planning
- Control & Quality
- Configuration Services
- Financial Management

DoD use of SOA
Computing Services

• Provide Adaptable Hosting Environments
  – Global facilities for virtual hosting to the “edge” for sharing applications, operating systems, and services.
  – Physical and virtual environments for data centers, applications and community-of-interest (COI) services.

• Distributed Computing Infrastructure
  – Computing, data storage, and shared spaces for data and information sharing.

• Shared Computing Infrastructure Resources
  – Access shared resources regardless of location or access device.

ISSUE
• How will data centers deliver high performance, high security, redundant connectivity?
Part 3

SOA Implementation: NCES
Current Scope of DISA/NCES

- Messaging
- Collaboration
- Mediation
- Content Discovery
- Content Delivery
- People Discovery
- Service Availability
- MetaData Registry

DoD use of SOA
– Monitoring of NCES web services on the GIG
– Service Oriented Architecture Foundation
– Content Discovery and Delivery
– Portal and Collaboration - NIPRNet and SIPRNet
– Joint Enterprise Directory Service (JEDS)
– Service security and certificate validation
– Metadata Registry

**ISSUE**
– Portal for NCES services launched from any portal
  • Concentrates on infrastructure, not applications.
  • Almost completely dependent on BEA software.
  • Intelligence Mission is just getting organized.
NCES Milestones

- Milestone C, March 2008
- Limited Operational Availability, April 2008
- Initial Operational Test and Evaluation, July 2008
- Initial Operational Capability, January 2009
- SOA Application Migration, 2010 - ?

ISSUE
- Is progress fast enough? Is there adequate investment?
- Which Project Plans anticipate NCES availability?
- MetaData Registry Inclusion into Projects is Unknown.
Part 4

What is Missing?
Transformation for SOA Migration

DoD Business Process Models

Middleware
For Transformation of Applications

Legacy Applications

DoD MetaData Directory

SOA

DoD use of SOA
SOA Middleware Vendors (Partial)

- Ab Initio
- BEA Systems
- IBM
- InterSystems
- Metastorm
- Oracle
- Pegasystems
- SAP
- Software AG
- Tibco
- Sun Microsystems
- Vignette
- VMWare
Requires Compliance with SOA Standards (Partial)

- Universal Description, Discovery, and Integration, **UDDI**. Defines the publication and discovery of web service implementations.

- The Web Services Description Language, **WSDL**, is an XML-based language that defines Web Services.

- **SOAP** is the Service Oriented Architecture Protocol. It is a key SOA in which a network node (the client) sends a request to another node (the server).

- The Lightweight Directory Access Protocol, or **LDAP** is protocol for querying and modifying directory services.

- The DoD I.T. Standards Registry makes **SOAP, WSDL, UDDI, WSS, WSRP, JSR168, WEBDEV** mandatory.
Example of Missing Application Services

- Provide Common End User Interface Tools
  - Application generators, test suites, error identification, application components, standard utilities, quality certification, etc.
- Common end-user Interface Tools.
  - E-mail environments, collaboration tools, information dashboards, and intranet portals, etc. These enable users to dynamically use and manipulate data and services on the network.
Part 5

Why SOA?
Transformation Through SOA

Customer, Integration

Equipment, Software.

Data, Communications.

Short-term Asset
>50% of Cost

Commodity
<20% of Cost

Long-term Asset
<30% of Cost

DoD use of SOA
**DoD SOA = >1,000 Billion Transactions / Hour**

<table>
<thead>
<tr>
<th>Generation</th>
<th>Period</th>
<th>Missions for National Security Systems</th>
<th>Interoperability: Number of Data Sources</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1955 - 1975</td>
<td>Automate Separate Applications</td>
<td>100</td>
</tr>
<tr>
<td>2</td>
<td>1975 - 1995</td>
<td>Automate Separate Processes</td>
<td>1,000</td>
</tr>
<tr>
<td>3</td>
<td>1995 - 2005</td>
<td>Integrate Processes within a Function</td>
<td>100,000</td>
</tr>
<tr>
<td>4</td>
<td>2005 - 2015</td>
<td>Integrate Functions within an Organization</td>
<td>10 Million</td>
</tr>
<tr>
<td>5</td>
<td>2015 - 2020</td>
<td>Innovate Processes As Needed</td>
<td>1 Billion</td>
</tr>
<tr>
<td>6</td>
<td>2025 -</td>
<td>Sense and Respond</td>
<td>1,000 Billion</td>
</tr>
</tbody>
</table>

**DoD use of SOA**
Summary

- SOA requires standardization.
- SOA requires discarding of obsolete assets.
- SOA is a driver in an “arms race”.
- SOA enables a weapon of Information Warfare.

- Current pace of SOA implementation is unsatisfactory.
- WW IV has already started.
- WW IV requires Information Superiority.
- SOA is necessary for DoD Information Superiority.
Prof. Paul A. Strassmann

E-mail: pstrassm@gmu.edu

Web: www.strassmann.com:

“What is a Service Oriented Architecture”