Software Sustainment Issues and Challenges
9 December 2015

Presented to:
2015 DoD Maintenance Symposium

Presented by:
Mr. Brian Marsh
Assistant Chief Engineer
(Certification & Mission Assurance)
Space and Naval Warfare Systems Command (SPAWAR)

Distribution Statement A. Approved for Public Release.
Distribution is unlimited (3 December 2015).
Software Within Today’s Navy Cyber Environment

Current State

- Flat, single network across enclaves
  - C4I, HM&E, Combat, Aviation
- No standardization in the implementation of security controls
- No authoritative end-to-end cyber baseline
- Inefficient, duplicative efforts
- Introduces seams & vulnerabilities…and larger attack vector
- Overly complex design
  - Difficult for sailors to operate and maintain
  - Perpetuates interoperability issues

The Collective Result of Individual Decisions

Attacks see a single network with seams

Today’s Infrastructure is Flat, Riddled with Seams and Flaws that are Easy to Exploit
Vision: A Single Navy Plan for Cyber

- Holistic enterprise cyber architecture
  - Layered, Defense-in-Depth approach that enables inheritance
  - Supports cyber SA across the network
- Mandatory implementation of standardized security controls
- Certified end-to-end baseline that meets cyber security requirements
- Streamlined investment
- Fewer seams and smaller cyber attack vector
- Easier for Sailors to operate and manage
- Greater interoperability

Upfront System of Systems Engineering Informs Cyber Investments Across the Enterprise
As the provider of a large portion of ships’ computing plant and C4ISR systems, SPAWAR plays a critical role in promoting more sustainable software.

In all aspects of development, specifications and standards that drive commonality and reduce complexity of implementations are key to delivering ships built for flexibility.

Key SPAWAR efforts that support Navy software sustainability:

- Promulgation of specifications and standards to address Information Technology and Information Assurance (i.e., Cyber) throughout lifecycle
- Development of common hosting environments to decouple applications from their operating environment
- Implementation of software development processes that reduce program risk and supportability costs
Information Technology (IT) / Information Assurance (IA) Technical Authority Board (TAB)

▼ Cross-Navy governance board for reviewing, adjudicating & endorsing IT & IA TA products for use throughout the Naval Enterprise

▼ The authority, responsibility, and accountability to establish, monitor and approve technical standards, tools, and processes in conformance with DoD and DON policy, requirements, architectures, and standards

SPAWAR-led TAB is the Cross-SYSCOM Governing Body for Enforcing IT/IA TA Discipline
Rapid Integration and Test Environment (RITE)

**Standard Software Process**

▼ Process and set of tools that expedites development, testing and delivery of software

▼ Provides greater visibility in the product process, catches major bugs earlier in development cycle and reduces risk to programs

▼ Enables faster, more frequent, more reliable delivery to the Fleet

<table>
<thead>
<tr>
<th>RITE Benefits</th>
<th>Increase</th>
<th>Decrease</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software Quality</td>
<td></td>
<td>Development Cost</td>
</tr>
<tr>
<td>System Reliability</td>
<td></td>
<td>Sustainment Cost</td>
</tr>
<tr>
<td>System Security</td>
<td></td>
<td>Time to Field</td>
</tr>
<tr>
<td>Engineering Productivity</td>
<td></td>
<td>Program Risk</td>
</tr>
</tbody>
</table>

Standards, Common Tools & Processes that Support Well-Integrated, Interoperable and Resilient Systems Also Promote Software Sustainability