Stories of Agile Acquisition

PluginFest – Results
Operationally Measured Acquisition

Eric Westreich,
PlugFest Consortium Lead
Esri Defense C2 Industry Manager
• Paul’s story (the engineer)
• Jeff’s Story (the advocate)
• Chris’ Story (the validator)
• Mike’s Story (the collaborator)
Real Solutions:
West 2014 PlugFest Technology Team

- Cyber
- Chip Positions
- Application Development
- Crisis Communication
- Workflow Development
- Presentation & Modeling

- Threat STOP
- Real-time
- Foundation Data
- Geospatial Viz & Analysis
- Presentation
- Enterprise Solutions
- Emergency Management

- esri
- IBM
- San Diego State University
- C4I Center
- LP3
- exactEarth
- virtualagility
- AtHoc
- Geocortex® by Latitude Geographics®
- simtable.com
## PlugFest Events Summary
(Over 1200 visitors/300 Collaborators)

<table>
<thead>
<tr>
<th>Challenge</th>
<th>Sponsor</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>Emergency Response - Haiti</td>
<td>AFCEA</td>
<td>AFCEA SD C4ISR Symposium</td>
</tr>
<tr>
<td>Opposed Maritime BattleGroup Transit</td>
<td>AFCEA</td>
<td>AFCEA SD C4ISR Symposium</td>
</tr>
<tr>
<td>Find, Fix, Finish Adversary</td>
<td>AFCEA Director USMC Intelligence</td>
<td>AFCEA Technet Southwest</td>
</tr>
<tr>
<td>Counter Narcotics</td>
<td>AFCEA DEA/DoD</td>
<td>AFCEA Technet South</td>
</tr>
<tr>
<td>Indications and warning of Cyber Threat</td>
<td>AFCEA US Army Cyber Command</td>
<td>AFCEA Technet East</td>
</tr>
<tr>
<td>Emergency Response for Bomb at Public Event</td>
<td>AFCEA USNI Los Angeles Sherriff's Dept Red Cross San Diego Police USMC</td>
<td>West 2013</td>
</tr>
</tbody>
</table>
# PlugFest Events Summary (Multiple Organizations)

<table>
<thead>
<tr>
<th>Challenge</th>
<th>Sponsor</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intelligent Common Operational Picture</td>
<td>Security Network</td>
<td>Security Summit</td>
</tr>
<tr>
<td>DI2E Architecture</td>
<td>OSD(I)/DI2E</td>
<td>DI2E PlugFest</td>
</tr>
<tr>
<td>Operational Cyber Logistics</td>
<td>AFCEA</td>
<td>AFCEA Cyber Symposium</td>
</tr>
<tr>
<td></td>
<td>US Cyber Command</td>
<td></td>
</tr>
<tr>
<td>Army Common Map API</td>
<td>DI2E</td>
<td>GMU Academic PlugFest</td>
</tr>
<tr>
<td></td>
<td>GMU</td>
<td></td>
</tr>
<tr>
<td>Basic Cyber Attack on U.S. Ports</td>
<td>InterAgency Board</td>
<td>IAB Meeting</td>
</tr>
<tr>
<td>Advanced Cyber Attack on U.S. Ports</td>
<td>AFCEA</td>
<td>West 2014</td>
</tr>
<tr>
<td></td>
<td>USNI</td>
<td></td>
</tr>
<tr>
<td></td>
<td>InterAgency Board</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SPAWAR</td>
<td></td>
</tr>
<tr>
<td>Common Map API</td>
<td>OSD(I)/DI2E</td>
<td>DI2E PlugFest</td>
</tr>
<tr>
<td>Sustained Communications</td>
<td>AFCEA</td>
<td>AFCEA Technet Augusta</td>
</tr>
<tr>
<td></td>
<td>US Army</td>
<td></td>
</tr>
</tbody>
</table>
Non-profit collaboration that believes that Government, Industry, and Academia working on the same problem, at the same time, together can deliver some technical capability better, faster and cheaper.
PlugFest Consortium Action
(Transitional Organization)

Investigate, Test, and Educate, agile Verification and Validation methods.

Facilitate and train others to Facilitate Agile V&V Events.

Find a permanent home for these functions.
• Mark’s Story (the educator)
Your Story
Agile is to Development, as PlugFest is to V&V

✓ What can I do today deliver better stuff faster?
✓ What will I do today that is outside of my comfort zone?
✓ What will I do to help teach others?
   - Place to discover and test theories, best practices, programs (virtual, scalable PlugFest lab)
   - Place to teach (virtual classroom)
   - Place to respond (virtual center of excellence)
“I must have heard “cool” a thousand times!”
Government Provided Problem: Cyber Attack on the Ports of Los Angeles & Long Beach

Hacker Goal: Disrupt 40% of the containerized cargo and material that enter the U.S.
Real Cyber Data
(Real Attacker, Anonymized Victim)
Every Application is part of the Common Operational Picture

The COP is shared awareness delivered
Question: What would take out loading capability at Ports of LA and Long Beach?

- Loading/Unloading Ships SCADA DoS Attack
- Crude Oil, Chlorine, Xylenol spills
Question: What is the most immediate impact?
Chlorine Plume

Fused, updating picture on PowerPoint, Excel, and Operations Dashboard
How to maintain Situational Awareness?

The ability to display relevant information rapidly and efficiently.
Question: How do we detect and defend sophisticated cyber-attacks against systems (including CIKR)?

Leverage Complex Event Processing to correlate data in real-time from a variety of monitoring sensors, providing alerts and automated responses.

Monitor hacktivists via social media
Coordinate key personnel

Malware file processing
Stateful behavioral analysis
Response plans

COP / dashboards
Question: How does the public know where to go to be safe?

Interactive Tactical Map
Question: How do we alert medical threat (red) in the plume, and evacuation (yellow) ahead of the plume?
Question: Attack on responders: how is response prevented? (EAS & ITS Attacks)
Question: How do you develop and implement courses of actions against cyber attack?
Question: How do we assign restoral tools across multiple platforms simultaneously?